Guide to Law Enforcement Processing 2
Scope and key definitions 3
Principles 9
Conditions for sensitive processing 16
Individual rights 19
Part 3 right of access 20
The right to rectification 26
The right to erasure and the right to restriction 30
Right not to be subject to automated decision-making 34
Manifestly unfounded and excessive requests 37
Part 3 right of access 44
Accountability and governance 50
Logging 51
Categorisation of individuals 53
Data protection by design and by default 55
Data protection impact assessments 56
Data protection officers 59
Manifestly unfounded and excessive requests 61
Personal data breaches 68
National security provisions 72
Penalties 80
International transfers 81
Resources 88
The Right of Access – Part 3 of the DPA 2018 91
Contents 93
What is the right of access in Part 3 of the DPA 2018? 96
How do we recognise a Part 3 subject access request (SAR) 102
What should we consider when responding to a Part 3 request? 116
How should we supply Part 3 information to the requester? 121
Can we restrict the right of access under Part 3? 127
What should we consider when acting as joint controllers? 138
What should we do if the Part 3 request involves information about other people? 143
What do we need to consider if personal information is processed by a court for law enforcement purposes? 150
Can the right of access be enforced under Part 3? 158

Guide to Law Enforcement Processing

The Guide to Law Enforcement Processing is part of our Guide to Data Protection. It is for those who have day-to-day responsibility for data protection in organisations with law enforcement functions.

It explains the data protection regime that applies to those authorities when processing personal data for law enforcement purposes. It covers part 3 of the Data Protection Act 2018 (DPA 2018), which is separate from the UK GDPR regime.

It explains each of the data protection principles, rights and obligations. It summarises the key points you need to know and answers frequently asked questions.

Where relevant, this guide also links to more detailed guidance and other resources, including ICO guidance and relevant European guidance published by the European Data Protection Board (EDPB). EDPB guidelines are no longer directly binding to the UK regime, but are included as a useful reference resource.

This section only covers processing for law enforcement purposes. You will need to read our Guide to the UK GDPR when processing for non-law enforcement purposes.

Scope and key definitions

At a glance

- Part 3 only applies to competent authorities (or their processors) processing for criminal law enforcement purposes.
- Processing for other general purposes such as HR will fall under the general processing regime in part 2 of the DPA 2018.
- It applies to processing of personal data, which is information about identifiable living individuals.
- Controllers determine how and why the data is processed. Processors process data on their behalf, but may share some accountability for the processing.
- There are additional rules which apply to 'sensitive processing' of some specified types of particularly sensitive data.

In brief

- Who does Part 3 apply to?
- What is a 'competent authority'?
- Are we processing for law enforcement purposes?
- What if we are processing for other general purposes?
- What happens if our purpose changes?
- How is personal data defined?
- What is a controller?
- What is sensitive processing?

Who does Part 3 apply to?

Part 3 only applies to competent authorities processing for law enforcement purposes. So, it applies, but is not limited, to:

- the police, criminal courts, prisons, non-policing law enforcement; and
- any other body that has statutory functions to exercise public authority or public powers for any of the law enforcement purposes.

The appropriate regime is based on the law that applies to the controller. So if you are a processor carrying out a law enforcement function on behalf of a competent authority, you will also be processing under this law enforcement processing regime.

Any processing carried out by a competent authority which is not for the **primary purpose** of law enforcement will be covered by the general processing regime under the UK

GDPR(read with Part 2 of the DPA 2018.

If you are a competent authority it is very likely that you are also processing personal data under the general processing regime. For example, this may include internal HR processes and procedures, as that processing isn't strictly for law enforcement purposes.

Identifying the correct regime is important as there are many key differences between the general processing regime and Part 3 of the DPA 2018, including differences on individuals' rights, lawful basis for processing and governance.

What is a 'competent authority'?

A competent authority means:

- a person specified in Schedule 7 of the DPA 2018; or
- any other person if, and to the extent that, they have statutory functions to exercise public authority or public powers for the law enforcement purposes.

You need to check whether you are listed as a competent authority in Schedule 7 of the DPA 2018.

If you are not listed in Schedule 7, you may still be a competent authority if you have a legal power to process personal data for law enforcement purposes. For example, local authorities who prosecute trading standards offences or the Environment Agency when prosecuting environmental offences.

> Relevant provisions in the DPA 2018 - See Section 30 and Schedule 7
> External link

Are we processing for law enforcement purposes?

If you are a competent authority, when you are deciding which regime applies, the key thing to consider is your **primary purpose** for the processing. This should help you identify whether the processing falls under the UK GDPR rules, or satisfies the criteria of the law enforcement purposes under Part 3 of the DPA 2018.

The law enforcement purposes are defined under section 31 of the DPA 2018 as:

> 'The prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'

So if you are a competent authority processing for one of those purposes, you should comply with the law enforcement processing regime.

Example

A police officer is called to a disturbance where allegations of assault have been made. The officer attends the scene using their body-worn camera. Witnesses are interviewed and this footage is recorded on the body-worn camera.

The footage is recorded and processed to investigate the crime. So the processing is carried out for the prevention, investigation, detection or prosecution of criminal offences. Part 3 of the DPA 2018 applies.

What if we are processing for other general purposes?

Even if you are a competent authority, in some circumstances, you may also process data for **general purposes,** such as for your own HR purposes. If processing is not for the law enforcement purposes, it will fall into the general processing regime in the UK GDPR read with and Part 2 of the DPA 2018 you should refer to our Guide to the UK GDPR.

Example

A police force want to obtain information from the public about their perception of the force in general. The results will help influence how the force engage with the public. They therefore conduct a survey to capture people's views.

Personal information is collected about individuals, but the primary purpose of the processing is to gain an insight into their opinions of the force. So the processing is not to prevent and detect crime.

In this case, the relevant regime is the general processing regime, and you should read our Guide to the GDPR.

What happens if our purpose changes?

You may begin processing information under one regime, but as circumstances progress and the purpose changes, the processing of the data will come under another regime or take place under both simultaneously.

You may initially be processing data for general administrative purposes, but as the situation changes you may identify elements of criminality. The processing would then come under Part 3 of the DPA 2018. It may be easier to identify a change in regime if the data is passed to a specialist team or department to continue the processing for a specific purpose. For example, a dedicated fraud unit may obtain information originally collected

under the general processing regime for the purposes of an investigation under Part 3 of the DPA 2018.

Likewise, in certain circumstances the processing of information by a competent authority may begin under the law enforcement processing regime in Part 3 of the DPA 2018, and as circumstances change, it may switch to the general processing regime. Some information may end up being processed for different purposes and under both regimes.

Any information that is being processed for law enforcement purposes must adhere to the governance requirements of Part 3 of the DPA 2018. These include logging requirements, categorisation and obligations about the principles and rights of individuals.

Example

A Police force is dealing with an internal disciplinary matter involving a member of staff. A complaint has been referred to a professional standards department about an officer's conduct. The complaint is not of a criminal matter.

The processing involves the use of data from various internal sources, such as HR. The primary purpose for processing the data is to investigate staff conduct and behaviour, so will be processed under the general processing regime.

As the investigation progresses, an element of criminality is discovered. The relevant data is then passed to a specific team. They will process the data to investigate the criminal aspects, so will need to comply with the law enforcement processing regime under Part 3 of the DPA 2018.

The HR department may still be processing some of the data for HR-related matters, and that will still be processed under the general processing regime.

Further reading

Read our guidance on:

Data sharing and reuse of data by competent authorities for non-law enforcement purposes

How is personal data defined?

Any information relating to an identified or identifiable **living** individual. An identifying characteristic could include a name, ID number or location data. You should treat such information as personal data even if it can only be potentially linked to a living individual.

Relevant provisions in the Act - See Section 1

External link

What is a controller?

A controller determines how and why personal data is processed. For the purposes of law enforcement, this will be a competent authority which is acting alone, or jointly with others.

If you are processing jointly with another competent authority, you must designate a specific controller to be the contact point for data subjects.

If you are a processor, you are processing personal data on behalf of the controller for the law enforcement purposes, but you could be sharing some accountability with controllers. This means that you could be liable for breaches. You need to review and revise your contracts to ensure that they reflect your new obligations.

Relevant provisions in the Act - See Section 32

External link

What is sensitive processing?

Sensitive processing is defined in section 35(8) as:

> (a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
>
> (b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
>
> (c) the processing of data concerning health;
>
> (d) the processing of data concerning an individual's sex life or sexual orientation.

Genetic data is personal data relating to the inherited or acquired characteristics of a person, eg an analysis of a biological sample.

Biometric data is personal data that is obtained through specific technical processing relating to physical, physiological or behavioural characteristics of a person. This processing enables you to identify a particular person, eg fingerprint data and facial recognition.

For more information on the rules about sensitive processing, see our guide pages on the principles and conditions for sensitive processing.

Relevant provisions in the Act - See Sections 35 and 205

External link

Principles

At a glance

- The six law enforcement data protection principles under Part 3, Chapter 2 of the DPA 2018 are the main responsibilities you should follow when processing personal data for law enforcement purposes.
- The principles are broadly the same as those in the UK GDPR, and are compatible so you can manage processing across the two regimes.
- There are no principles relating to individuals' rights or overseas transfers of personal data – these are addressed in Part 3 of the DPA 2018 separately.
- Transparency requirements are not as strict as in the UK GDPR, due to the potential to prejudice an ongoing investigation in certain circumstances.
- You must be able to demonstrate overall compliance with all of the law enforcement data protection principles.

In brief

- What are the principles?
- Why are the principles important?
- What is the first principle about?
- What about sensitive processing?
- What safeguards are required for sensitive processing?
- What is the second principle about?
- What are principles three, four and five about?
- What is the sixth principle about?

What are the principles?

Part 3, Chapter 2 of the DPA 2018 sets out six key principles which are your main responsibilities when processing personal data for the law enforcement purposes.

The principles are broadly the same as those in the UK GDPR, and are compatible so you can manage your processing across the two regimes.

The first data protection principle
Processing of personal data for any of the law enforcement purposes must be lawful and fair.

The second data protection principle
The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and;

Personal data collected must not be processed in a manner that is incompatible with the purpose for which it was originally collected.

The third data protection principle
Personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

The fourth data protection principle
Personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and;

Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

The fifth data protection principle
Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.

Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

The sixth data protection principle
Personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

Section 34(3) adds that:

> The controller in relation to personal data is responsible for, and must be able to demonstrate, compliance with this Chapter.

Why are the principles important?

The principles guide and inform the processing of personal data for the law enforcement regime under Part 3 of the DPA 2018.

They don't give hard and fast rules, but rather embody the spirit of the law enforcement regime – and as such there are very limited exceptions.

Compliance with the spirit of these key principles is therefore a fundamental building block for good data protection practice. It is also key to your compliance with the detailed provisions of Part 3.

Failure to comply with the principles may leave you open to substantial fines. Section 157(2)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of monetary penalties. This could mean a penalty of up to £17.5 million, or 4% of your total worldwide annual turnover, whichever is higher.

What is the first principle about?

The first data protection principle says that any processing for the law enforcement purposes must be lawful and fair. Lawfulness and fairness are well established requirements of data protection law.

For the processing to be lawful, section 35(2) says that it must be "based on law". This means that the processing is authorised by either statute, common law or royal prerogative, or by or under any other rule of law. You must identify a legal basis that provides a sufficiently clear, precise and foreseeable lawful justification to process personal data for the law enforcement purposes. The necessary legal basis may be found in more than one statute or other source of law.

Example

Part 5 of the Police and Criminal Evidence Act 1984 confers statutory authority for the taking and retention of DNA and fingerprints (this applies to England and Wales).

The Domestic Violence Disclosure Scheme relies on the Police's common law powers to disclose information where it is necessary to do so to prevent crime.

The processing must also have a lawful basis under data protection legislation. Section 35(2) explains that the processing of personal data for any of the law enforcement purposes must be either necessary for the performance of a task carried out for law enforcement purposes by a competent authority, or based on consent.

You need to be aware that any processing you carry out for the law enforcement purposes must be necessary. This does not mean that processing always has to be essential. However, it must be a targeted and proportionate way of achieving your purpose. This

lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means.

It is not enough to argue that processing is necessary because you have chosen to operate in a particular way. The question is whether the processing is a necessary for the stated purpose.

In terms of consent under Part 3, this has the same high standard of consent as that in the UK GDPR. This means consent must be freely given and it must be unambiguous and involve a clear affirmative action (an opt-in). Individuals also must be able to easily withdraw consent. Further guidance on consent can be found in the Guide to UK GDPR page.

There may be limited circumstances where you obtain consent from the individual whose personal data you are processing. However, in the context of law enforcement processing, consent may often not be appropriate as a lawful basis.

"Fairness" generally means you must not process personal data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned. It also requires you to be, where appropriate, clear and open with individuals about how you use their information, in keeping with their reasonable expectations.

What about sensitive processing?

ICO guidance explains the meaning of 'necessary' as a targeted and proportionate way of achieving your purpose under Article 6 UK GDPR. Processing for a law enforcement purpose may for example, depending on each case, be 'necessary' if it delivers that purpose more effectively, for the benefit of society.

However, as a law enforcement authority, the information you process will often be sensitive. When it is, you must be able to demonstrate that processing for a law enforcement purpose is either based on consent or alternatively, is **strictly necessary** and satisfies one of the conditions in Schedule 8 of the DPA 2018.

'Strictly necessary', as required in some sections of Part 3 DPA 2018, imposes a more exacting standard than 'necessary', and in practice calls for a more rigorous justification for why you are processing the information.

The standard should be more exacting for the processing of sensitive information because it carries greater risk, and may have a greater impact on individuals' rights. As such, this requires higher levels of protection and safeguards. Whether the processing of sensitive information for any of the law enforcement purposes is 'strictly necessary' should depend upon the facts of each case.

In the view of the ICO, we expect 'strictly necessary' under Part 3 DPA 2018 to mean that enhanced consideration and extra care should be taken to:

- ensure that the processing of sensitive information is specific in nature and dependent on the specified law enforcement purpose;
- clearly demonstrate why there are reasonably no less intrusive means of achieving the same purpose; and
- clearly demonstrate how such processing will be effective in meeting the specified law enforcement purposes.

Sensitive processing is defined in the law enforcement provisions as:

> (a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
>
> (b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
>
> (c) the processing of data concerning health;
>
> (d) the processing of data concerning an individual's sex life or sexual orientation.

Genetic data is personal data relating to the inherited or acquired characteristics of a person, eg an analysis of a biological sample.

Biometric data is personal data that is obtained through specific processing relating to physical, physiological or behavioural characteristics of a person. This processing enables you to identify a particular person, eg fingerprints and facial recognition.

Given the sensitivity surrounding such processing, you are required to meet at least one of the conditions set out in Schedule 8 of the DPA 2018.

What safeguards are required for sensitive processing?

If you are carrying out sensitive processing based on the consent of a data subject, or based on another specific condition in Schedule 8 of the DPA 2018, you must have an appropriate policy document in place.

This document must explain:

- your procedures for ensuring compliance with the law enforcement data protection principles; and
- your policies on the retention and erasure of this data.

You must retain this policy from the time you begin sensitive processing until six months after it has ended. You must review and update it where appropriate and make it available to the Information Commissioner upon request without charge.

So, to recap, sensitive processing must be:

- based on the consent of the data subject; or
- strictly necessary for the law enforcement purpose and based on a Schedule 8 condition.

In addition, in either case you must have an appropriate policy document in place.

Our template appropriate policy document shows the kind of information this should contain.

What is the second principle about?

The second principle is about maintaining the purpose for processing personal data. Specific requirements about the purpose being **specified, explicit and legitimate** are introduced, meaning that any processing under Part 3 of the DPA 2018 must be for the defined law enforcement purposes. You cannot process for a purpose that is incompatible with the original reason and justification for processing.

> The Crown Prosecution Service could process personal data in connection with the prosecution of a criminal offence, whereas the Police working alongside the prosecutor would only be processing the personal data in connection with the investigation of the offence.

What are principles three, four and five about?

The third principle requires that the personal data you are processing is **adequate, relevant and not excessive**. This means the data must be limited to what is necessary for the purpose(s) you are processing it.

The fourth data protection principle is about accuracy. It sets out that you should take every reasonable step to correct inaccurate data. In addition, **as far as possible**, you need to be able to distinguish between personal data that is based on factual data and that which is based on a matter of opinion or assessment, such as a witness statement.

A new requirement is that again, where relevant, and as far as possible, you need to be able to distinguish data between different categories of individuals, such as suspects; individuals who have been convicted; victims and witnesses. You only categorise information under Part 3 that is relevant to your investigation, and other unused data falls under the general processing regime.

The fifth principle requires that you do not keep personal data for longer than is necessary for the purpose you originally collected it for. No specific time periods are given but you need to conduct regular reviews to ensure that you are not storing for longer than necessary for the law enforcement purposes.

What is the sixth principle about?

The sixth principle requires you to have technical and organisational measures in place to ensure that you protect data with an appropriate level of security. This is the same as under the UK GDPR and Part 2 of the DPA 2018

"Appropriate security" includes "protection against unauthorised or unlawful processing and against accidental loss, destruction or damage".

> Relevant provisions in the DPA 2018 - see Sections 34,35, 36, 37, 38, 39, 40, 41, 42, 157 and Schedule 8
> External link

Conditions for sensitive processing

Latest updates - last updated 09 March 2023

> **09 March 2023** - We have shortened a description of "strictly necessary" in the "At a glance" section for "Conditions for sensitive processing". Further detail can now be found under the "What about sensitive processing?" section instead.

At a glance

The conditions for sensitive processing in Schedule 8 of the Act are:

- necessary for judicial and statutory purposes – for reasons of **substantial public interest**;
- necessary for the administration of justice;
- necessary to protect the vital interests of the data subject or another individual;
- necessary for the safeguarding of children and of individuals at risk;
- personal data already in the public domain (manifestly made public);
- necessary for legal claims;
- necessary for when a court acts in its judicial capacity;
- necessary for the purpose of preventing fraud; and
- necessary for archiving, research or statistical purposes.

Again, you must be able to demonstrate that the processing is **strictly necessary** and satisfy one of the conditions in Schedule 8 or is based on consent.

In brief

- What are the conditions?
- What is an appropriate policy document?
- What are judicial and statutory purposes/administration of justice?
- When is processing appropriate for individual's vital interests?
- What about personal data already in the public domain?
- When does processing relate to safeguarding of children and of individuals at risk?
- What about legal claims and judicial acts?
- When can data be processed for preventing fraud?
- What about archiving?

What are the conditions?

When undertaking 'sensitive processing', in order to comply with the first principle, you must either have consent for processing or be able to satisfy one of the conditions in Schedule 8. Consent should not always be a default condition as it may not be appropriate in the circumstances. You will also need an appropriate policy document in place.

What is an appropriate policy document?

An appropriate policy document must explain:

(a) your procedures for ensuring compliance with the law enforcement data protection principles; and

(b) your policies on the retention and erasure of this data.

Our template appropriate policy document shows the kind of information this should contain.

What are judicial and statutory purposes/administration of justice?

The sensitive processing must be necessary for the administration of justice, or the exercise of a function conferred 'on a person' by enactment. This covers a constable and other competent authorities.

In addition, in order to satisfy this condition, you must be able to demonstrate that the processing is necessary for reasons of substantial public interest.

When is processing appropriate for individual's vital interests?

This condition only applies in cases of life or death, such as if you disclose an individual's medical history to a hospital's A&E department who are treating them after a serious road accident. Data protection law should not be a barrier to processing data in these circumstances.

When does processing relate to safeguarding of children and of individuals at risk?

This condition is met in cases where consent is not appropriate because the individual is under 18 or at risk, but the processing is necessary for reasons of substantial public interest, and is to protect them from harm or to protect their well-being.

What about personal data already in the public domain?

This condition applies if the data subject has deliberately made the information public.

What about legal claims and judicial acts?

This condition is met if the processing is necessary for the establishment, exercise or defence of a legal claim or whenever a court is acting in its judicial capacity.

When can data be processed for preventing fraud?

You should use this condition if the processing is necessary for the purposes of preventing fraud. If it involves sharing data with organisations that do not fall within the definition of a competent authority, the processing needs to comply with the UK GDPR, and you need to have a lawful basis for sharing the data.

What about archiving?

You can use this condition if processing is necessary for archiving in the public interest; for scientific or historical research purposes, or for statistical purposes. However, you cannot use it if it will result in decisions being made that effect a particular individual, or is likely to cause substantial damage or substantial distress to an individual.

> Relevant provisions in the Act - See Schedule 8
> External link

Individual rights

Part 3, Chapter 3 of the Act provides the following individual rights:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure or restrict processing; and
- the right not to be subject to automated decision-making.

Certain rights under the UK GDPR, such as the right to object and the right to data portability, do not exist in Part 3 of the Act. Further, there are exemptions and restrictions that can, in some circumstances, be legitimately applied to prevent individuals from exercising rights.

It is important to note that subject access rights and the rights to rectification, erasure and restriction do not apply to the processing of **'relevant personal data'** in the course of a criminal investigation or criminal proceedings.

'Relevant personal data' means personal data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority.

Access to 'relevant personal data' is governed by the appropriate legislation covering the disclosure of information in criminal proceedings, such as (in England and Wales) the Criminal Procedure and Investigations Act 1996.

This provision only applies if the judge or other judicial authority is the controller and the relevant personal data is contained in a judicial decision or in other documents which are created during a criminal investigation or proceedings and made by or on behalf of the judge or judicial authority. For example, the 'relevant personal data' may be contained in judge's notes.

You must communicate any information in clear and plain language that you are required to provide in Part 3. It is also your duty more generally to assist individuals to exercise their rights.

Similar to the UK GDPR, the Act includes further provisions for individuals to exercise their rights through raising a complaint with the Information Commissioner, or taking matters to court.

The next sections explain each of these in more detail.

Part 3 right of access

Latest updates - last updated 10 February 2023

> **10 February 2023** - We have published detailed guidance on the Part 3 right of access, and updated our in-brief guidance to reflect this.

At a glance

- People have a legal right to access their personal information. This means that you **should** provide them with a copy of their personal information, where possible, and other supplementary information.
- This is known as a subject access request, or 'SAR'.
- People can make SARs verbally or in writing, including via social media.
- A third party can also make a SAR on behalf of another person.
- If you are a competent authority processing personal information for law enforcement purposes, you **must** deal with the SAR under Part 3.
- You **must** deal with requests for unstructured manual data under the UK GDPR, and not Part 3.
- You do not have to disclose information processed by a court in connection with criminal matters to respond to a SAR.
- In most circumstances, you **must not** charge a fee to deal with a request.
- You **must** provide the requested information without delay, and at the latest within one month. You **must not** extend this time limit for any reason.
- You **should** perform a reasonable search for this information.
- You **must** provide the information in an accessible, concise and intelligible format.
- You **must** disclose the information in a manner that ensures appropriate security.
- You **could** refuse to provide the information if a Part 3 restriction applies or if the request is manifestly unfounded or excessive.

Checklists

Preparing for Part 3 subject access requests

□ We know how to recognise a request and we understand when the right of access applies.

□ We understand what information is being used for law enforcement purposes, and when to use Part 3 to deal with the SAR.

□ We have a policy for recording verbal requests.

□ We understand what steps we need to take, if necessary, to verify the requester's identity.

□ We understand that we must respond to requests within one month.

□ We understand when we can restrict the right of access and are aware of the information we still need to provide to people when we do so.

□ We understand the nature of the supplementary information we must provide to respond to a subject access request.

□ We have suitable information management systems in place to allow us to locate and retrieve information efficiently.

Complying with Part 3 subject access requests

□ We have processes in place to ensure that we respond to a request without undue delay and within one month of receipt.

□ We understand how to perform a reasonable search for the information.

□ We understand what we should consider if a third party makes a request on someone's behalf.

□ We understand how to deal with requests for personal information contained within logs of information.

□ We understand how to deal with requests for unstructured manual data.

□ We understand that we must provide the information in a concise, intelligible and easily accessible form, using clear and plain language.

□ We understand that we should generally provide people with a copy of their personal information and other supplementary information.

□ We have processes in place for when we may consider restricting someone's right of access, and have a system for recording our reasons.

□ We understand what we should consider if a request includes information about others.

□ We understand that, in circumstances where we are joint controllers, we must have joint arrangements in place. These must set out the responsibilities of each joint controller, and designate one of the joint controllers as the "contact point"

for SARs.

□ We can deliver the information securely and in the correct format.

In brief

- What is the right of access in Part 3 of the DPA 2018?
- How do we recognise a Part 3 subject access request (SAR)?
- What should we consider when responding to a Part 3 request?
- How should we supply Part 3 information to the requester?
- Can we restrict the right of access under Part 3?
- What should we consider when acting as joint controllers?
- What should we do if the Part 3 request involves information about other individuals?
- What do we need to consider if a court processes personal data for law enforcement purposes?
- Can the ICO enforce the right of access under Part 3?
- Part 3 right of access in more detail

What is the right of access in Part 3 of the DPA 2018?

The UK GDPR does not apply to personal information used for any of the law enforcement purposes. There is a separate regime in Part 3 of the DPA 2018 which gives people a right to access their personal information used for a law enforcement purpose.

The right of access in Part 3, commonly known as subject access, gives people the right to access their personal information, as well as other supplementary information. It helps people to understand how and why you are using their data, and check you are doing so lawfully.

How do we recognise a Part 3 subject access request (SAR)?

Someone can make a Part 3 SAR verbally or in writing, including on social media. A request is valid if it is clear that the person is asking for their own personal information. They do not need to use a specific form of words, refer to legislation or direct the request to a specific contact.

Before responding to a SAR, you **must** determine whether you are using the personal information for any of the law enforcement purposes. If you are a competent authority, and your primary purpose for processing the information is for one of the law enforcement purposes, you **must** deal with the SAR under Part 3.

What should we consider when responding to a Part 3 request?

You **must** comply with a SAR without undue delay and at the latest within one month of receiving the request. The time limit begins the day after you receive the request. You **must not** extend the time limit for any reason. While you may ask the person to clarify their request, you **must not** 'stop the clock' after doing so. You **must** still comply with the request within the deadline.

Under Part 3, you **must** keep logs of information about your processing activities.

Unstructured personal data is manual information that is not, or is not intended to form, part of a "filing system". Unstructured manual data obtained for law enforcement purposes is not included in the Part 3 processing regime. If you receive a SAR for this type of personal information you will need to treat it as SAR under the UK GDPR.

How should we supply Part 3 information to the requester?

People have the right to access their personal information. Where possible, you **should** provide with them a copy of their personal information, and other supplementary information (which largely corresponds with the information that you should provide in a privacy notice).

You **must** respond to requests in writing, and provide the information in a concise, intelligible, and easily accessible format using clear and plain language. You **could** provide the information in its existing format, if this is the most accessible form. For example, where you cannot convey the full context and meaning of the information solely in writing. This may include providing secure access to CCTV footage, or audio recordings. You do not have to create transcripts to respond to a request, if you do not already have them.

In certain circumstances you **could** provide the person with access to their information, rather than providing them with a copy. Our detailed guidance further explains these circumstances.

Can we restrict the right of access under Part 3?

Yes – but only in specific circumstances.

People have the right to obtain confirmation of whether or not you process their information, and to access it.

You may restrict these rights, in full or in part, if it is necessary and proportionate in order to:

- avoid obstructing an official or legal inquiry, investigation or procedure;
- avoid prejudice to the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;

- protect national security; or
- protect the rights and freedoms of others.

In considering whether to apply a restriction, you **must** also consider the person's fundamental rights and interests. You **must** provide them with any information you do not need to restrict access to.

What should we consider when acting as joint controllers?

Where two or more competent authorities jointly determine the purposes and means of the processing of personal information, they are acting as joint controllers.

If you are acting as a joint controller, you **must** ensure that:

- you have an arrangement in place with your fellow joint controllers, which clearly and transparently sets out each of your responsibilities under Part 3, including how you deal with SARs; **and**
- you specify a contact point for people, which is one of the joint controllers.

Joint controllers **must**, in their joint arrangements, name one of the joint controllers as the contact point. You **must not** appoint a third party as the contact point, or have more than one contact point.

The joint arrangements **must** set out very clearly the duties of each joint controller in relation to SARs.

What should we do if the Part 3 request involves information about other people?

You **should** consider first whether it is possible to comply with the request without disclosing information that identifies another person.

If this is not possible, you should consider whether it is reasonable to apply a restriction. In reaching this decision, you **must** balance the rights and interests of the person making the request with the rights and freedoms of the other person.

If you can demonstrate, on balance, that applying a restriction is necessary and proportionate to protect the rights and freedoms of the other person, then you **could** refuse to provide the information.

Our detailed guidance provides further information on what you need to consider in these circumstances.

What do we need to consider if a court processes personal data for law enforcement purposes?

People do not have a right to access their personal data by making a SAR if it is contained in:

- a judicial decision; or
- in another document created by or on behalf of a court or other judicial authority in connection with,
  - a criminal investigation; or
  - criminal proceedings, including proceedings for the sentencing of an offender.

The DPA 2018 describes such information as "relevant personal data".

Can the ICO enforce the right of access under Part 3?

Yes. In appropriate cases, the ICO may take action against a controller or processor if they fail to comply with data protection legislation. The ICO will exercise these enforcement powers in accordance with our Regulatory Action Policy.

If you fail to comply with a SAR, the requester may apply for a court order requiring you to comply or to seek compensation. It is a matter for the court to decide, in each particular case, what action to take.

If you are a joint controller, you are only liable to the extent you are responsible for the specific action in question, under the terms of the joint arrangements.

> Relevant provisions in the legislation - See DPA 2018, Part 3
> External link

In more detail – ICO guidance

We have produced more detailed guidance on the Part 3 right of access.

The right to rectification

At a glance

- Individuals have the right to have personal data rectified.
- You can rectify personal data if it is inaccurate or incomplete.
- You must rectify any inaccurate personal data that relates to the individual without undue delay, and in any event within one month.

In brief

- When should we rectify personal data?
- What do we need to do to comply?
- What if the request is manifestly unfounded or excessive?
- How long do we have to comply?
- When can we limit the provision of information?

When should we rectify personal data?

You must rectify inaccurate personal data when it becomes apparent, or, if an individual requests it. If personal data is identified as inaccurate as a matter of fact, or incomplete, you must seek to amend this by rectifying or completing the data. If you are unable to correct it, you could provide a supplementary statement to rectify personal data which is inaccurate if appropriate. In circumstances such as policing, you can keep accurate records of allegations made, even if the allegations are unfounded.

Example

The right to rectification applies, in particular, to matters of fact. For example, there may be inaccuracies in the details of a criminal conviction held on the Police National Computer. An individual may receive a copy of their criminal record and request that an incorrect entry for Grievous Bodily Harm is corrected to Actual Bodily Harm, or vice versa, to reflect the correct conviction. The controller may restrict the right to rectification if, for example, it obstructs an investigation, such as a request to rectify the content of a witness statement.

If you need to maintain personal data for the purposes of evidence, you must restrict its processing (instead of rectifying it). There is further information in the next section about restricting the processing of personal data.

If this happens, an individual may raise a complaint with the Information Commissioner.

What do we need to do to comply?

An individual can make a request for rectification verbally or in writing. Therefore, it is good practice to have a policy for recording details of the requests you receive, including those made by telephone or in person. You may wish to check with the requester that you have understood their request as this can help avoid later disputes. We also recommend that you keep a log of verbal requests.

If you have reasonable doubts about the identity of an individual, you can request more information to confirm their identity. You can put dealing with the request on hold until you receive further information to establish their identity.

Your request for verification should be reasonable and proportionate, taking into consideration the nature of the personal data you hold and your relationship with the individual.

If you have disclosed the personal data in question to third parties, you must inform them of the rectification. The third parties also have to rectify the information they hold. You must also inform the competent authority (if any) where the inaccurate personal data originated from.

If you refuse a request for rectification, you must tell the individual, informing them of their right to raise a complaint with the Information Commissioner or taking matters to court.

What if the request is manifestly unfounded or excessive?

If requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

You have to be able to demonstrate how a request is manifestly unfounded or excessive.

How long do we have to comply?

You must respond to the request without delay and at the latest within one calendar month, from the first day after the request was received.

Example

If you receive a request on 30 June the time limit will start on 1 July and the deadline will be 1 August.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

For practical purposes if a consistent number of days is required (eg for a computer system), you should adopt a 28-day period to ensure compliance is always within a calendar month.

When can we limit the provision of information?

If you receive a request for rectification, you must inform the individual in writing whether you have granted the request; and if you have refused, the reasons why, as well as the process for raising a complaint with the Information Commissioner or taking matters to court.

You may limit the provision of information to:

- avoid obstructing an official or legal inquiry, investigation or procedure;
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security; or
- protect the rights and freedoms of others.

You need to justify any restriction you apply as necessary and proportionate. Again, you should also consider whether refusal or rectification in itself prejudices an ongoing investigation, as it may well indicate to an individual that you are processing their personal data.

You still need to inform the individual about their right to raise a complaint with the Information Commissioner or take matters to court.

In addition, you should keep a record of your decisions and provide this reasoning to the Information Commissioner, if required.

> Relevant provisions in the Act - See sections 46, 48, 52 and 53, Chapter 3

External link

The right to erasure and the right to restriction

At a glance

- Individuals also have the right to request the deletion or removal of their personal data.
- Individuals also have a right to 'block' or restrict processing of their personal data.

In brief

The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals also have the right to restrict the processing of their personal data.

The Act defines the restriction of processing as the 'marking of stored personal data with the aim of limiting its processing for the future'.

When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that you respect the restriction in future.

Restriction could involve measures such as transferring data to a separate system, or limiting the access through the use of passwords and other access controls.

- What do we need to consider when deciding if the right to erasure applies?
- What do we need to do to comply with requests for erasure or restriction?
- What if the request is manifestly unfounded or excessive?
- How long do we have to comply?
- When should we restrict processing?
- When can we limit the provision of information?

What do we need to consider when deciding if the right to erasure applies?

Individuals have a right to have personal data erased or to restrict its processing.

You must erase personal data without undue delay if:

- the processing of the personal data will infringe **the data protection principles**;
- you do not meet safeguards for **archiving** and processing of **sensitive personal data**; or
- you have a **legal obligation** to erase the data.

We recognise that complete deletion of personal data in electronic systems can often be problematic, but you should ensure that you have adequate systems and storage media in place to comply with an individual's request for erasure. If deletion is not technically possible, you should at least take steps to put the personal data 'beyond use'.

What do we need to do to comply with requests for erasure or restriction?

The Act does not specify how to make a request, so an individual can do so verbally or in writing. Therefore, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request as this can help avoid later disputes. We also recommend that you keep a log of verbal requests.

If you have reasonable doubts about the identity of an individual, you can request more information to confirm their identity. You can delay dealing with the request until you receive further information to establish their identity.

Your request for information to verify a requester's identity should be reasonable and proportionate, taking into consideration the nature of the personal data you hold and your relationship with the individual.

If you have disclosed the personal data in question to third parties, you must inform the third party about the erasure or restriction of the personal data. The third parties will also have to erase or restrict the personal data they hold.

You must tell an individual if you are not going to erase or rectify the personal data they have requested that you amend. You must also inform them of their right to raise a complaint with the Information Commissioner or take the matter to court.

What if the request is manifestly unfounded or excessive?

If requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

You have to be able to demonstrate how a request is manifestly unfounded or excessive.

How long do we have to comply?

You must respond to the request without delay and at the latest within one calendar month, from the first day after the request was received.

Example

If you receive a request on 30 June the time limit will start on 1 July and the deadline will be 1 August.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

For practical purposes if a consistent number of days is required (eg for a computer system), you should adopt a 28-day period to ensure compliance is always within a calendar month.

When should we restrict processing?

You are required to restrict the processing of personal data for the law enforcement purposes in two situations:

- If you must maintain personal data for the purposes of evidence.
- If an individual contests the accuracy of personal data but it is not possible to be certain about its accuracy.

If restriction is based on the latter, you should inform the individual before you lift the restriction.

Example

A local authority is investigating a suspect for benefit fraud. As part of this investigation, factually inaccurate personal data about the suspect (such as an age/ethnicity) has been received from a third party. However this inaccurate record needs to be retained as evidence to account for how the local authority first carried out the investigation and the source of this information. They should not erase or rectify this information, but restrict it as it forms evidence against the suspect. They should not process this inaccurate personal data for any other purpose.

When can we limit the provision of information?

If you receive a request for rectification, you must inform the individual in writing whether you have granted the request; and if you have refused, the reasons why, as well as the process for raising a complaint with the Information Commissioner or taking matters to court.

You may limit the provision of information where it is necessary and proportionate to:

- avoid obstructing an official or legal inquiry, investigation or procedure;
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security; or
- protect the rights and freedoms of others.

Any restriction you apply needs to be justified as necessary and proportionate. In deciding on proportionality it is important to balance the rights of the data subject against the harm disclosure would cause. You can only limit the information you provide to the extent that it would prejudice the purposes stated above.

There is also an obligation to inform the data subject when this limitation is in place, explaining its existence and the reasons unless providing this information itself undermines the purpose of imposing the restriction. You still need to inform the individual about recourse to the Information Commissioner and the Court process.

You should keep a record of your decisions and provide this reasoning to the Information Commissioner if required.

Relevant provisions in the Act - See sections 47, 48, 52 and 53, Chapter 3

External link

Right not to be subject to automated decision-making

At a glance

- Part 3 provides safeguards for individuals against the risk that a potentially damaging decision is taken by **solely** automated means, ie without human intervention.
- You may not take a significant decision based solely on automated processing unless that decision is required or authorised by law. A 'qualifying significant decision' is defined as a decision which significantly affects or produces an adverse legal effect on an individual and is authorised by law.
- Currently, solely automated decision-making that leads to an adverse outcome is rarely used in the law enforcement context and is unlikely to have many operational implications.

In brief

- When does the right apply?
- How do we comply?

When does the right apply?

Individuals have the right **not to be subject to a decision** when:

- it is based on automated processing; and
- it produces an adverse legal effect or significantly affects the individual.

You must ensure that individuals are able to:

- obtain human intervention;
- express their point of view; and
- obtain an explanation of the decision and challenge it.

To qualify as human intervention, you must ensure that you carefully analyse the decision and consider all the available input and output data, rather than just a token review. This should be carried out by someone who has the authority and competence to change the decision.

This right does not specifically refer to profiling. However, profiling is defined in section 33 as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

- performance at work;
- economic situation;
- health;
- personal preferences;
- interests;
- reliability;
- behaviour;
- location; or
- movements.

Profiling and automated decision-making can be combined activities of the same process, or can be carried out separately. There may be cases of automated decisions made with (or without) profiling and profiling which may take place without making automated decisions. This right will therefore apply to any profiling which involves some form of automated processing.

The right does not apply when a decision does not have an adverse legal or similarly significant effect on someone.

Example

An automated processing system could include an IT database of criminal records or prosecution histories, where data is input or accessed by staff via automated means.

'Automated decision making' only comes into play where the controller takes a 'significant' decision based solely upon automated processing, often without any human interaction. This is a decision that produces an adverse legal effect concerning the individual or otherwise affects the individual.

How do we comply?

You should inform an individual if you make a 'qualifying significant decision' about them.

The individual has one month to request for you to review the decision, or take a new decision not based solely on automated means. You must consider the request including any information provided by the individual. You need to respond to the individual within one month of receipt of their request and outline the steps you have taken as well as the outcome.

The DPA 2018 does not specify how an individual must make a request, so they can make it verbally or in writing. Therefore, it is good practice to have a policy for recording details

of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes.

Relevant provisions in the DPA 2018 - See Sections 49, 50, 52 and 53, Chapter 3
External link

Other resources

Toolkit for organisations considering using data analytics

Manifestly unfounded and excessive requests

Latest updates - last updated 10 February 2023

> **10 February 2023** - We have updated our Part 3 guidance on manifestly unfounded and excessive requests to align with our new policy lines on this topic in the UK GDPR right of access guidance.

At a glance

- Under Part 3 of the DPA 2018, people have rights of access, rectification, erasure and restriction of their personal data. They also have the right for their personal data to not be subject to automated decision-making.
- You **could** refuse to respond to a request if it is manifestly unfounded or excessive.
- Alternatively, you **could** charge a reasonable fee for dealing with the request.
- You **must** demonstrate why it is manifestly unfounded or excessive.

Checklists

Responding to manifestly unfounded and excessive requests

□ We understand when we can refuse a request and are aware of the information we need to provide to people when we do so.

□ We understand the considerations we need to account for when deciding if a request is manifestly unfounded or excessive.

In brief

- What types of requests can we consider as manifestly unfounded or excessive?
- What general considerations should we take into account when deciding if a request is manifestly unfounded or excessive?
- What does manifestly unfounded mean?
- What does manifestly excessive mean?
- What should we do if we refuse to comply with a request?
- When can you charge a fee?

What types of requests can we consider as manifestly unfounded or excessive?

People have the right to request:

- access to their personal data;
- rectification of their personal data;
- restriction of the processing of their personal data;
- erasure of their personal data; and
- not to be subject to automated decision-making.

For further information about these rights, please see our Guide to Law Enforcement Processing.

If you process personal data for law enforcement purposes and you consider a request exercising any of these rights as manifestly unfounded or excessive, you **could** refuse to comply with the request.

Alternatively, you **could** charge a reasonable fee to deal with the request (see When can you charge a fee?).

What general considerations should we take into account when deciding if a request is manifestly unfounded or excessive?

You **should** determine whether a request is manifestly unfounded or excessive on a case-by-case basis. You **should** also consider the individual circumstances.

Whilst there may be characteristics that are indicative of a manifestly unfounded or excessive request, you should only use these as a guide. You **must not** presume that a request is manifestly unfounded or excessive just because someone has previously submitted manifestly unfounded or excessive requests.

The inclusion of the word "manifestly" means it must be obvious or clear that the request is unfounded or excessive. You **must** have evidence as to why you consider a request to be manifestly unfounded or excessive. You must be able to explain the reasons for your decision to the person and, if asked, to the Information Commissioner's Office (ICO).

What does manifestly unfounded mean?

A request may be manifestly unfounded if the person clearly has no intention to exercise their right or if the request is malicious in intent. They may also use the request to harass an organisation, with no real purpose other than to cause disruption. The term 'manifestly' indicates that organisations should provide evidence which demonstrates why the request is unfounded.

Factors that may indicate a manifestly unfounded request include where:

- the person explicitly states, in the request itself or in other communications, that they intend to cause disruption;
- the request makes unsubstantiated or false accusations against you or specific employees which are clearly prompted by malice;
- the person is targeting a particular employee against whom they have a personal grudge;
- the person makes a request but then offers to withdraw it in return for some sort of benefit from the organisation; or
- the person systematically or frequently sends different requests to you as part of a campaign with the intention of causing disruption, eg once a week.

This is not a simple tick list that automatically means a request is manifestly unfounded. You **should** consider a request in its own context, and consider all the circumstances. The onus is on you to demonstrate that a request is manifestly unfounded.

You **should** consider the particular situation and whether the person genuinely wants to exercise their rights. If they do want to exercise their rights, it is unlikely that the request is manifestly unfounded. In most cases, use of aggressive or abusive language does not, in itself, demonstrate a manifestly unfounded request.

Example

A person is unhappy with the outcome of a complaint to a regulator. They post online that they plan to make a request for the company to delete their information every day, until the employee that dealt with their complaint is fired.

You have already responded to their first erasure request. It is clear that their intention is to threaten or disrupt your organisation. You refuse these further requests on the grounds that they are manifestly unfounded.

What does manifestly excessive mean?

To determine whether a request is manifestly excessive, you **should** consider whether it is clearly or obviously unreasonable. You **should** base this on whether the request is proportionate, when balanced with the burden or costs involved in dealing with the requests.

This means taking into account all the circumstances of the request, including:

- the nature of the information the request is about;
- the context of the request and the circumstances of the relationship between you and the person;

- whether a refusal to carry out the request or even acknowledge that you hold relevant information may cause substantive damage to the person, such as an adverse impact on their rights. You **should** think about rights broadly by considering any aspect of a person's life;
- your available resources;
- if the request largely repeats previous requests and there has not been a reasonable interval since the last request;
- whether it largely overlaps with other requests (although if it is about a separate set of information, it is unlikely to be excessive); or
- where you have already provided a copy of the information to the person by alternative means.

In most cases, a request is not excessive just because the request covers a large amount of information, even if you find it a burden. As noted above, you **should** consider all the circumstances of the request. If it is a request for access, you **could** also consider asking them for more information to help you locate the information they are looking for.

A repeat request may not be excessive if a reasonable amount of time has passed since their last request. You should consider the following when deciding whether a reasonable amount of time has passed:

- the nature of the data – this could include whether it is particularly sensitive;
- whether the circumstances of the request have changed, for example, can you provide access to information you previously restricted, now that the circumstances have changed?; and
- how often you alter the data.

If it is unlikely that there have been any changes to the information between requests, you **could** decide you do not need to respond to the same request twice.

If you have deleted information since the last request, you **should** let the requester know.

If you have collected new information since their last request then it may not be an excessive request (at least not for the new information).

Requests about the same issue are not always excessive. Someone may have legitimate reasons for making requests that repeat the content of previous requests. For example, if the organisation did not handle previous requests properly, or if a response to a previous request provided someone with new information that they were not previously aware of, prompting a new request. However, in other circumstances, a request which effectively repeats the substance of a previous request may be excessive. This depends on the circumstances.

A request may be excessive if someone makes a new request before you have had the opportunity to address an earlier request. However, this is only the case if the substance of the new request repeats some of the previous request. It is unlikely to be excessive if the overlapping request is about a separate set of information.

A request for information is not automatically excessive just because the information was previously made available as part of the criminal justice system. However, if a person has already received exactly the same information through an alternative statutory disclosure mechanism, this may be a factor to consider in deciding whether a request is excessive. In deciding whether such a request is excessive you **should** take into account the wider circumstances of the request, including:

- Have you provided exactly the same information as the person has now requested?
- Does the person already know this?
- What would be the likely impact on the person's rights, freedoms and interests, if you refused the request? Would they suffer substantive damage?

The rights that are impacted may vary in the circumstances. The amount of weight you attach to the person's rights, freedoms or legitimate interests will depend on how compelling or trivial they are.

For further guidance on considering how people's rights may be affected, see 'What rights and interests may be impacted by restricting an individual's right of access?'. For further information on handling requests where you have already provided the information, please see 'Do we have to respond to the SAR if the person has an alternative means of accessing their information?'. These pieces of guidance are about the right of access. However the principles are also relevant to determining the impact to other Part 3 rights.

Example

One month ago, you responded to a person's subject access request for their information, which included their conviction history. Since then, they have made a new request for their information and asked you to include their conviction history again. Since their last request, the only new information you have collected covers a call to your complaint department.

You consider the amount of time you need to provide all the information, including their conviction history which contains a lot of documents, compared to only providing new information. You decide that it would be excessive to provide all the information, especially because of:

- the overlap in information;

- the volume of information in their conviction history; and
- the time elapsed since the last request.

You refuse to respond to the whole request again, and tell the person that their request is excessive. However, you do provide them with the new information that you have collected since their last request.

What should we do if we refuse to comply with a request?

If you refuse to comply with a request, you **must** inform the person of:

- the reasons why you are not complying with their request;
- their right to make a complaint to the ICO; and
- their ability to seek to enforce this right through a judicial remedy.

As mentioned above, if you believe a request is manifestly unfounded or excessive you must be able to demonstrate this to the person and, if asked, to the ICO.

When can you charge a fee?

You **could** charge a reasonable fee if you decide that a request is manifestly unfounded or excessive, but you choose to respond to it. However, you are not required to charge a fee, and you can still refuse to deal with the request (on the grounds that it is unreasonable or excessive). This is the case even if the person tells you they are willing to pay a fee.

If you decide to charge a fee, you **must** notify the requester and explain why. You do not need to take further action in response to the request until you receive the fee. The time limit for responding to the request begins once you have received the fee. You **should** request the fee as soon as possible and, at the latest, within one month of receiving the request. You **should not** unnecessarily delay requesting it until you are nearing the end of the one month time limit. If you decide on a reasonable fee, you must be able to justify the cost, in case the requester makes a complaint to the ICO.

Section 53(4) allows for the Secretary of State to specify limits on the fees that organisations may charge to deal with a manifestly unfounded or excessive request by way of regulations. However, at present there are no regulations in place. As such, it is your responsibility as an organisation to ensure that you charge a reasonable rate.

For further guidance on the factors that you **should** consider when determining a reasonable fee and how you should respond to a request when you are charging a fee, you should follow our UK GDPR right of access guidance – 'Can we charge a fee?'.

Example

An accused person repeatedly makes SARs for a file containing personal information about their arrest. You have given them the same file before, and you have not collected any more information since their initial request. The request is excessive, but you decide to respond to the request because you think they may have lost the file.

You tell the person you are charging them a fee for this information, based on administration costs. Once you receive the fee, you provide the information within one calendar month.

Relevant provisions in Part 3 of the DPA 2018 – The Part 3 provisions for manifestly unfounded and excessive requests are listed in Chapter 3, section 53

External link

Part 3 right of access

At a glance

- People have a legal right to access their personal information. This means that you **should** provide them with a copy of their personal information, where possible, and other supplementary information.
- This is known as a subject access request, or 'SAR'.
- People can make SARs verbally or in writing, including via social media.
- A third party can also make a SAR on behalf of another person.
- If you are a competent authority processing personal information for law enforcement purposes, you **must** deal with the SAR under Part 3.
- You **must** deal with requests for unstructured manual data under the UK GDPR, and not Part 3.
- You do not have to disclose information processed by a court in connection with criminal matters to respond to a a SAR.
- In most circumstances, you **must not** charge a fee to deal with a request.
- You **must** provide the requested information without delay, and at the latest within one month. You **must not** extend this time limit for any reason.
- You **should** perform a reasonable search for this information.
- You **must** provide the information in an accessible, concise and intelligible format.
- You **must** disclose the information in a manner that ensures appropriate security.
- You **could** refuse to provide the information if a Part 3 restriction applies or if the request is manifestly unfounded or excessive.

Checklists

Preparing for Part 3 subject access requests

□ We know how to recognise a request and we understand when the right of access applies.

□ We understand what information is being used for law enforcement purposes, and when to use Part 3 to deal with the SAR.

□ We have a policy for recording verbal requests.

□ We understand what steps we need to take, if necessary, to verify the requester's identity.

□ We understand that we must respond to requests within one month.

□ We understand when we can restrict the right of access and are aware of the information we still need to provide to people when we do so.

□ We understand the nature of the supplementary information we must provide to respond to a subject access request.

□ We have suitable information management systems in place to allow us to locate and retrieve information efficiently.

Complying with Part 3 subject access requests

□ We have processes in place to ensure that we respond to a request without undue delay and within one month of receipt.

□ We understand how to perform a reasonable search for the information.

□ We understand what we should consider if a third party makes a request on someone's behalf.

□ We understand how to deal with requests for personal information contained within logs of information.

□ We understand how to deal with requests for unstructured manual data.

□ We understand that we must provide the information in a concise, intelligible and easily accessible form, using clear and plain language.

□ We understand that we should generally provide people with a copy of their personal information and other supplementary information.

□ We have processes in place for when we may consider restricting someone's right of access, and have a system for recording our reasons.

□ We understand what we should consider if a request includes information about others.

□ We understand that, in circumstances where we are joint controllers, we must have joint arrangements in place. These must set out the responsibilities of each joint controller, and designate one of the joint controllers as the "contact point" for SARs.

□ We can deliver the information securely and in the correct format.

In brief

- What is the right of access in Part 3 of the DPA 2018?
- How do we recognise a Part 3 subject access request (SAR)?
- What should we consider when responding to a Part 3 request?
- How should we supply Part 3 information to the requester?
- Can we restrict the right of access under Part 3?
- What should we consider when acting as joint controllers?
- What should we do if the Part 3 request involves information about other individuals?
- What do we need to consider if personal data is processed by a court for law enforcement purposes?
- Can the right of access be enforced under Part 3?
- Part 3 right of access in more detail

What is the right of access in Part 3 of the DPA 2018?

The UK GDPR does not apply to personal information used for any of the law enforcement purposes. There is a separate regime in Part 3 of the DPA 2018 which gives people a right to access their personal information used for a law enforcement purpose.

The right of access in Part 3, commonly known as subject access, gives people the right to access their personal information, as well as other supplementary information. It helps people to understand how and why you are using their data, and check you are doing so lawfully.

How do we recognise a Part 3 subject access request (SAR)?

Someone can make a Part 3 SAR verbally or in writing, including on social media. A request is valid if it is clear that the person is asking for their own personal information.

They do not need to use a specific form of words, refer to legislation or direct the request to a specific contact.

Before responding to a SAR, you **must** determine whether you are using the personal information for any of the law enforcement purposes. If you are a competent authority, and your primary purpose for processing the information is for one of the law enforcement purposes, you **must** deal with the SAR under Part 3.

What should we consider when responding to a Part 3 request?

You **must** comply with a SAR without undue delay and at the latest within one month of receiving the request. The time limit begins the day after you receive the request. You **must not** extend the time limit for any reason. While you may ask the person to clarify their request, you **must not** 'stop the clock' after doing so. You **must** still comply with the request within the deadline.

Under Part 3, you **must** keep logs of information about your processing activities.

Unstructured personal data is manual information that is not, or is not intended to form, part of a "filing system". Unstructured manual data obtained for law enforcement purposes is not included in the Part 3 processing regime. If you receive a SAR for this type of personal information you will need to treat it as SAR under the UK GDPR.

How should we supply Part 3 information to the requester?

People have the right to access their personal information. Where possible, you **should** provide with them a copy of their personal information, and other supplementary information (which largely corresponds with the information that you should provide in a privacy notice).

You **must** respond to requests in writing, and provide the information in a concise, intelligible, and easily accessible format using clear and plain language. You **could** provide the information in its existing format, if this is the most accessible form. For example, where you cannot convey the full context and meaning of the information solely in writing. This may include providing secure access to CCTV footage, or audio recordings. You do not have to create transcripts to respond to a request, if you do not already have them.

In certain circumstances you **could** provide the person with access to their information, rather than providing them with a copy. Our detailed guidance further explains these circumstances.

Can we restrict the right of access under Part 3?

Yes – but only in specific circumstances.

People have the right to obtain confirmation of whether or not you process their information, and to access it.

You may restrict these rights, in full or in part, if it is necessary and proportionate in order to:

- avoid obstructing an official or legal inquiry, investigation or procedure;
- avoid prejudice to the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security; or
- protect the rights and freedoms of others.

In considering whether to apply a restriction, you **must** also consider the person's fundamental rights and interests. You **must** provide them with any information you do not need to restrict access to.

What should we consider when acting as joint controllers?

Where two or more competent authorities jointly determine the purposes and means of the processing of personal information, they are acting as joint controllers.

If you are acting as a joint controller, you **must** ensure that:

- you have an arrangement in place with your fellow joint controllers, which clearly and transparently sets out each of your responsibilities under Part 3, including how you deal with SARs; **and**
- you specify a contact point for people, which is one of the joint controllers.

Joint controllers **must**, in their joint arrangements, name one of the joint controllers as the contact point. You **must not** appoint a third party as the contact point, or have more than one contact point.

The joint arrangements **must** set out very clearly the duties of each joint controller in relation to SARs.

What should we do if the Part 3 request involves information about other people?

You **should** consider first whether it is possible to comply with the request without disclosing information that identifies another person.

If this is not possible, you should consider whether it is reasonable to apply a restriction. In reaching this decision, you **must** balance the rights and interests of the person making the request with the rights and freedoms of the other person.

If you can demonstrate, on balance, that applying a restriction is necessary and proportionate to protect the rights and freedoms of the other person, then you **could** refuse to provide the information.

Our detailed guidance provides further information on what you need to consider in these circumstances.

What do we need to consider if a court processes personal data for law enforcement purposes?

People do not have a right to access their personal data by making a SAR if it is contained in:

- a judicial decision; or
- in another document created by or on behalf of a court or other judicial authority in connection with,
  - a criminal investigation; or
  - criminal proceedings, including proceedings for the sentencing of an offender.

The DPA 2018 describes such information as "relevant personal data".

Can the ICO enforce the right of access under Part 3?

Yes. In appropriate cases, the ICO may take action against a controller or processor if they fail to comply with data protection legislation. The ICO will exercise these enforcement powers in accordance with our Regulatory Action Policy.

If you fail to comply with a SAR, the requester may apply for a court order requiring you to comply or to seek compensation. It is a matter for the court to decide, in each particular case, what action to take.

If you are a joint controller, you are only liable to the extent you are responsible for the specific action in question, under the terms of the joint arrangements.

> Relevant provisions in the legislation - See DPA 2018, Part 3
> External link

> **In more detail – ICO guidance**
>
> We have produced more detailed guidance on the Part 3 right of access.

Accountability and governance

You are expected to put into place comprehensive but proportionate governance measures. Good practice tools that the ICO has championed for a long time such as privacy impact assessments and privacy by design are legally required in certain circumstances that pose a risk to the rights and freedoms of individuals.

Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many will already have good governance measures in place.

What is the accountability principle?

Part 3, Chapter 2 of the Act requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility as data controller.

How can we demonstrate that we comply?

You must implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.

In addition, you must:

- maintain relevant documentation on your processing activities;
- where appropriate, appoint a data protection officer; and
- implement measures that meet the principles of data protection by design and data protection by default.

Such measures could include:

- data minimisation;
- pseudonymisation;
- transparency, where appropriate;
- creating and improving security features on an ongoing basis; or
- data protection impact assessments where appropriate.

Toolkit for organisations considering using data analytics

For organisations
File

Logging

At a glance

If you operate automated processing systems (any IT database), you must keep logs for **at least** the following processing actions:

- Collection
- Alteration
- Consultation
- Disclosure (including transfers)
- Combination
- Erasure

In brief

What is the purpose of logging?

It is to enable you to monitor and audit internal processing within any automated processing systems you use, and to know which third parties you have shared data with so that you can inform them of changes to the data should you need to. In addition, logging enables you to monitor systems for inappropriate access and/or disclosure of data, to verify the lawfulness of any processing, and to ensure the integrity and security of personal data.

> **Example**
>
> If an officer or member of police staff is suspected of inappropriately accessing the Police National Computer to check on a neighbour, family member or friend, the logging should show what was available to them at the time, which will assist with any potential internal investigations.

The law enforcement provisions do not include a definition of 'automated processing system' however it is interpreted to mean any system that undertakes processing by automated means, and is likely to involve human interaction (for example input of or access to data) at some point.

If you operate automated processing systems (any IT database), you must keep logs for **at least** the following processing actions:

- Collection

- Alteration
- Consultation
- Disclosure (including transfers)
- Combination
- Erasure

It is important that you do not record the data itself in your logs of erasure, as there is no need to retain a duplicate record of what you have erased. The requirement is to produce metadata which displays, for example, what a specific person on a specific date erased. The 'what' does not have to detail the content of the record/information that has been deleted – it can simply record that record *X* was updated by a specific individual.

Logs must also record, where possible, the identity of the person who accessed (consulted) the data, the reason for the access, and the date and time of any associated action. You should also record the identity of any recipients, in cases of disclosure – this is particularly important as you will need to inform the recipients if you delete, amend or restrict the processing of this data following a request from the individual.

There are however limitations to what you can use logs for. Any logs that you keep for the above processing actions may only be used for one or more of the following purposes:

- to verify the lawfulness of processing;
- to assist with self-monitoring by the controller or the processor, including the conduct of internal disciplinary proceedings;
- to ensure the integrity and security of personal data; or
- the purposes of criminal proceedings.

You (and any associated processor) may be required to make these records available to the Information Commissioner upon request.

> ### Relevant provisions of the Act - See section 62, Chapter 4
> External link

Categorisation of individuals

At a glance

When processing personal data for the any of the law enforcement purposes, you must provide, **where relevant and as far as possible**, a clear distinction between different categories of personal data, such as people who are:

- suspected of having committed, or about to commit, a criminal offence (suspects);
- convicted of a criminal offence;
- individuals who are, or are suspected of being, victims of a criminal offence (victims); or
- individuals who are witnesses, or can provide information, about a criminal offence (witnesses).

In brief

Under the fourth principle, you must ensure that any personal data you process for law enforcement purposes is accurate and, where necessary, up to date.

In all areas of policing and criminal justice, it is highly likely that any processing of personal data will involve different categories of data subject. When processing personal data for the any of the law enforcement purposes, you must provide, **where relevant and as far as possible**, a clear distinction between different categories of personal data, such as people who are:

- suspected of having committed, or about to commit, a criminal offence (suspects);
- convicted of a criminal offence;
- individuals who are, or are suspected of being, victims of a criminal offence (victims); or
- individuals who are witnesses, or can provide information, about a criminal offence (witnesses).

There may be instances where an individual falls under more than one of these categories. For example an individual may be both a victim and a witness in a certain case, or indeed an offender in one case and victim/witness in another. You will therefore be required, where relevant and as far as possible, to have processes and procedures in place to distinguish between such categories.

Example

If a competent authority obtains a large dataset as part of an investigation, the authority only needs to categorise the personal data that is relevant to the investigation. In practice, this will be data that has operational value to a criminal investigation, rather than any other collateral data that they have also acquired.

The competent authority will only categorise the information under Part 3 **where relevant** to the investigation, and any other unused data will fall under the general provisions of the UK GDPR/ Part 2 of the Act.

It is important to note that any unused personal data is also subject to strict retention periods.

You must also distinguish, so far as possible, any personal data based on facts from personal data based on personal assessment. In essence, this is the ability to distinguish between fact and opinion.

For example, statements by victims and witnesses containing personal data are based on the subjective perceptions of the person making the statement. These statements are not always verifiable and are subject to challenge during the legal process. In such cases, the requirement for accuracy does not apply to the content of the statement but simply that a specific statement has been made.

The requirement to keep personal data up to date must also be viewed in this context. If an individual's conviction is overturned on appeal, police must amend their records. However, they will not retrospectively alter a witness statement even if the court has found it to be unreliable.

Relevant provisions of the Act - See Section 38, chapter 2

External link

Data protection by design and by default

At a glance

- You have a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities.
- Privacy by design has always been an implicit requirement of data protection that the ICO has consistently championed.
- The ICO has published guidance on privacy by design and default within the Guide to the UK GDPR.

In brief

What is data protection by design?

Under the UK GDPR and Part 3 of the Act, you have a general obligation to implement appropriate technical and organisational measures to show that you have considered and integrated the principles of data protection into your processing activities.

If you are processing personal data for law enforcement purposes, you must implement these measures by default, to ensure that you only process personal data for a specified and necessary purpose.

In particular, you must ensure that by default, you put safeguards in place to prevent personal data being made available to an indefinite number of people without an individual's intervention.

Example

An authority responsible for courts and tribunals are building new IT systems for storing or accessing personal data. Prior to any live use, the authority is required to review their privacy and data protection compliance and perceived risks from the start of the project, rather than adding on such considerations at the end. This process could involve undertaking a Data Protection Impact Assessment (DPIA).

Relevant provisions of the Act - See Section 57, Chapter 4

External link

Data protection impact assessments

At a glance

- A data protection impact assessment (DPIA) is 'an assessment of the impact of the envisaged processing operations on the protection of personal data'.
- You must carry out a DPIA before you process personal data when the processing is likely to result in a high risk to the rights and freedoms of individuals.
- The ICO has produced guidance and screening checklists about DPIAs that you may wish to adopt.

In brief

- What is a data protection impact assessment?
- When do we need to conduct a DPIA?
- How do we carry out a DPIA?
- When do we need to send our DPIA to the ICO?

What is a data protection impact assessment?

Data protection impact assessments or DPIAs (previously known as privacy impact assessments or PIAs) are a tool that can help you identify the most effective way to comply with your data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow you to identify and fix problems at an early stage, reducing the associated costs and damage to your reputation which might otherwise occur.

When do we need to conduct a DPIA?

You must carry out a DPIA before you process personal data when the processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions that have legal effects, or similarly significant effects, on individuals;
- large scale processing of special categories of data or personal data relation to criminal convictions or offences;
- using new technologies (for example surveillance systems).

You must take into account the nature, scope, context and purposes of the processing when deciding whether or not it is likely to result in a high risk to individuals' rights and freedoms.

How do we carry out a DPIA?

A DPIA must contain:

- at least a general description of your processing operations and the purposes;
- an assessment of the risks to the rights and freedoms of individuals;
- the measures envisaged to address those risks;
- the safeguards, security measures and mechanisms in place to ensure you protect the personal data; and
- a demonstration of how you are complying with Part 3 of the Act, taking into account the rights and legitimate interests of the data subjects and any other people concerned.

When do we need to send our DPIA to the ICO?

If you have carried out a DPIA that identifies a high risk, and you cannot take any measures to reduce this risk, you need to consult the ICO. You cannot go ahead with the processing until you have done so.

The focus is on the 'residual risk' after any mitigating measures have been taken. If your DPIA identified a high risk, but you have taken measures to reduce this risk so that it is no longer a high risk, you do not need to consult the ICO.

The Information Commissioner will respond within **six weeks**. This timescale may increase by a further month, depending on the complexity of the processing you intend to carry out.

For detail on how to submit a DPIA to the ICO, please see 'Do we need to consult the ICO?'.

Example

A police force is considering using a commercially available drone system for surveillance purposes. By conducting a DPIA prior to any purchase of the equipment or processing taking place, the force can establish whether or not the equipment offers adequate security for the recording, and if the use of the system is proportionate or poses a high risk to the rights and freedoms of any individuals.

If they discover high risks after conducting a DPIA, and cannot easily mitigate any residual risk, the police force should consider consulting with the Information Commissioner for further guidance or approval.

Relevant provisions of the Act - See Sections 64, 65, Chapter 4

External link

Data protection officers

At a glance

- Data protection officers (DPOs) assist you to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner.
- The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.
- A DPO can be an existing employee or externally appointed.
- In some cases several organisations can appoint a single DPO between them.
- DPOs can help you demonstrate compliance and are part of the enhanced focus on accountability.

In brief

- When do we need to appoint a data protection officer for Law Enforcement processing?
- What are the tasks of the DPO?
- What does the Part 3 of the Act say about employer duties?
- Can we allocate the role of DPO to an existing employee?
- Does the DPO need specific qualifications?

When do we need to appoint a data protection officer for Law Enforcement processing?

Under the Part 3 of the Act, you must appoint a data protection officer (DPO) unless you are a court, or other judicial authority acting in a judicial capacity.

You may appoint a single data protection officer to act for a group of controllers, taking into account their structure and size.

Regardless of whether the UK GDPR or Part 3 of the Act obliges you to appoint a DPO, you must ensure that relevant staff have sufficient skills and expertise to discharge your obligations.

What are the tasks of the DPO?

The DPO's minimum tasks are defined in Part 3, Chapter 4 of the Act:

- to inform and advise the controller, its employees, and any associated processors about their obligations to comply with the UK GDPR and other relevant data protection laws

such as Part 3 of the Act;
- to monitor compliance with data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits; and
- to be the first point of contact for the Information Commissioner and for individuals whose data is processed (employees, customers etc).

What does the Part 3 of the Act say about employer duties?

You must ensure that:

- the DPO reports to the highest relevant management level of your organisation – ie board level;
- the DPO operates independently, and is not dismissed or penalised for performing their task, however a DPO can still be dismissed or penalised for misconduct or negligence relating to their task; and
- you provide adequate resources to enable DPOs to meet their obligations under UK GDPR or Part 3 of the Act.

Can we allocate the role of DPO to an existing employee?

Yes. As long as the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests.

You can also contract out the role of DPO externally.

Does the DPO need specific qualifications?

The UK GDPR or Part 3 of the Act does not specify the precise credentials a data protection officer is expected to have.

It does require that they should have professional experience and knowledge of data protection law. This should be proportionate to the type of processing you carry out, taking into consideration the level of protection the personal data requires.

> **Relevant provisions of the Act - See Sections 69 to 71, Chapter 4**
> External link

Manifestly unfounded and excessive requests

At a glance

- Under Part 3 of the DPA 2018, people have rights of access, rectification, erasure and restriction of their personal data. They also have the right for their personal data to not be subject to automated decision-making.
- You **could** refuse to respond to a request if it is manifestly unfounded or excessive.
- Alternatively, you **could** charge a reasonable fee for dealing with the request.
- You **must** demonstrate why it is manifestly unfounded or excessive.

Checklists

Responding to manifestly unfounded and excessive requests

□ We understand when we can refuse a request and are aware of the information we need to provide to people when we do so.

□ We understand the considerations we need to account for when deciding if a request is manifestly unfounded or excessive.

In brief

- What types of requests can we consider as manifestly unfounded or excessive?
- What general considerations should we take into account when deciding if a request is manifestly unfounded or excessive?
- What does manifestly unfounded mean?
- What does manifestly excessive mean?
- What should we do if we refuse to comply with a request?
- When can you charge a fee?

What types of requests can we consider as manifestly unfounded or excessive?

People have the right to request:

- access to their personal data;
- rectification of their personal data;
- restriction of the processing of their personal data;
- erasure of their personal data; and
- not to be subject to automated decision-making.

For further information about these rights, please see our Guide to Law Enforcement Processing.

If you process personal data for law enforcement purposes and you consider a request exercising any of these rights as manifestly unfounded or excessive, you **could** refuse to comply with the request.

Alternatively, you **could** charge a reasonable fee to deal with the request (see When can you charge a fee?).

What general considerations should we take into account when deciding if a request is manifestly unfounded or excessive?

You **should** determine whether a request is manifestly unfounded or excessive on a case-by-case basis. You **should** also consider the individual circumstances.

Whilst there may be characteristics that are indicative of a manifestly unfounded or excessive request, you should only use these as a guide. You **must not** presume that a request is manifestly unfounded or excessive just because someone has previously submitted manifestly unfounded or excessive requests.

The inclusion of the word "manifestly" means it must be obvious or clear that the request is unfounded or excessive. You **must** have evidence as to why you consider a request to be manifestly unfounded or excessive. You must be able to explain the reasons for your decision to the person and, if asked, to the Information Commissioner's Office (ICO).

What does manifestly unfounded mean?

A request may be manifestly unfounded if the person clearly has no intention to exercise their right or if the request is malicious in intent. They may also use the request to harass an organisation, with no real purpose other than to cause disruption. The term 'manifestly' indicates that organisations should provide evidence which demonstrates why the request is unfounded.

Factors that may indicate a manifestly unfounded request include where:

- the person explicitly states, in the request itself or in other communications, that they intend to cause disruption;
- the request makes unsubstantiated or false accusations against you or specific employees which are clearly prompted by malice;
- the person is targeting a particular employee against whom they have a personal grudge;

- the person makes a request but then offers to withdraw it in return for some sort of benefit from the organisation; or
- the person systematically or frequently sends different requests to you as part of a campaign with the intention of causing disruption, eg once a week.

This is not a simple tick list that automatically means a request is manifestly unfounded. You **should** consider a request in its own context, and consider all the circumstances. The onus is on you to demonstrate that a request is manifestly unfounded.

You **should** consider the particular situation and whether the person genuinely wants to exercise their rights. If they do want to exercise their rights, it is unlikely that the request is manifestly unfounded. In most cases, use of aggressive or abusive language does not, in itself, demonstrate a manifestly unfounded request.

Example

A person is unhappy with the outcome of a complaint to a regulator. They post online that they plan to make a request for the company to delete their information every day, until the employee that dealt with their complaint is fired.

You have already responded to their first erasure request. It is clear that their intention is to threaten or disrupt your organisation. You refuse these further requests on the grounds that they are manifestly unfounded.

What does manifestly excessive mean?

To determine whether a request is manifestly excessive, you **should** consider whether it is clearly or obviously unreasonable. You **should** base this on whether the request is proportionate, when balanced with the burden or costs involved in dealing with the requests.

This means taking into account all the circumstances of the request, including:

- the nature of the information the request is about;
- the context of the request and the circumstances of the relationship between you and the person;
- whether a refusal to carry out the request or even acknowledge that you hold relevant information may cause substantive damage to the person, such as an adverse impact on their rights. You **should** think about rights broadly by considering any aspect of a person's life;
- your available resources;

- if the request largely repeats previous requests and there has not been a reasonable interval since the last request;
- whether it largely overlaps with other requests (although if it is about a separate set of information, it is unlikely to be excessive); or
- where you have already provided a copy of the information to the person by alternative means.

In most cases, a request is not excessive just because the request covers a large amount of information, even if you find it a burden. As noted above, you **should** consider all the circumstances of the request. If it is a request for access, you **could** also consider asking them for more information to help you locate the information they are looking for.

A repeat request may not be excessive if a reasonable amount of time has passed since their last request. You should consider the following when deciding whether a reasonable amount of time has passed:

- the nature of the data – this could include whether it is particularly sensitive;
- whether the circumstances of the request have changed, for example, can you provide access to information you previously restricted, now that the circumstances have changed?; and
- how often you alter the data.

If it is unlikely that there have been any changes to the information between requests, you **could** decide you do not need to respond to the same request twice.

If you have deleted information since the last request, you **should** let the requester know.

If you have collected new information since their last request then it may not be an excessive request (at least not for the new information).

Requests about the same issue are not always excessive. Someone may have legitimate reasons for making requests that repeat the content of previous requests. For example, if the organisation did not handle previous requests properly, or if a response to a previous request provided someone with new information that they were not previously aware of, prompting a new request. However, in other circumstances, a request which effectively repeats the substance of a previous request may be excessive. This depends on the circumstances.

A request may be excessive if someone makes a new request before you have had the opportunity to address an earlier request. However, this is only the case if the substance of the new request repeats some of the previous request. It is unlikely to be excessive if the overlapping request is about a separate set of information.

A request for information is not automatically excessive just because the information was previously made available as part of the criminal justice system. However, if a person has already received exactly the same information through an alternative statutory disclosure mechanism, this may be a factor to consider in deciding whether a request is excessive. In deciding whether such a request is excessive you **should** take into account the wider circumstances of the request, including:

- Have you provided exactly the same information as the person has now requested?
- Does the person already know this?
- What would be the likely impact on the person's rights, freedoms and interests, if you refused the request? Would they suffer substantive damage?

The rights that are impacted may vary in the circumstances. The amount of weight you attach to the person's rights, freedoms or legitimate interests will depend on how compelling or trivial they are.

For further guidance on considering how people's rights may be affected, see 'What rights and interests may be impacted by restricting an individual's right of access?'. For further information on handling requests where you have already provided the information, please see 'Do we have to respond to the SAR if the person has an alternative means of accessing their information?'. These pieces of guidance are about the right of access. However the principles are also relevant to determining the impact to other Part 3 rights.

Example

One month ago, you responded to a person's subject access request for their information, which included their conviction history. Since then, they have made a new request for their information and asked you to include their conviction history again. Since their last request, the only new information you have collected covers a call to your complaint department.

You consider the amount of time you need to provide all the information, including their conviction history which contains a lot of documents, compared to only providing new information. You decide that it would be excessive to provide all the information, especially because of:

- the overlap in information;
- the volume of information in their conviction history; and
- the time elapsed since the last request.

You refuse to respond to the whole request again, and tell the person that their request is excessive. However, you do provide them with the new information

that you have collected since their last request.

What should we do if we refuse to comply with a request?

If you refuse to comply with a request, you **must** inform the person of:

- the reasons why you are not complying with their request;
- their right to make a complaint to the ICO; and
- their ability to seek to enforce this right through a judicial remedy.

As mentioned above, if you believe a request is manifestly unfounded or excessive you must be able to demonstrate this to the person and, if asked, to the ICO.

When can you charge a fee?

You **could** charge a reasonable fee if you decide that a request is manifestly unfounded or excessive, but you choose to respond to it. However, you are not required to charge a fee, and you can still refuse to deal with the request (on the grounds that it is unreasonable or excessive). This is the case even if the person tells you they are willing to pay a fee.

If you decide to charge a fee, you **must** notify the requester and explain why. You do not need to take further action in response to the request until you receive the fee. The time limit for responding to the request begins once you have received the fee. You **should** request the fee as soon as possible and, at the latest, within one month of receiving the request. You **should not** unnecessarily delay requesting it until you are nearing the end of the one month time limit. If you decide on a reasonable fee, you must be able to justify the cost, in case the requester makes a complaint to the ICO.

Section 53(4) allows for the Secretary of State to specify limits on the fees that organisations may charge to deal with a manifestly unfounded or excessive request by way of regulations. However, at present there are no regulations in place. As such, it is your responsibility as an organisation to ensure that you charge a reasonable rate.

For further guidance on the factors that you **should** consider when determining a reasonable fee and how you should respond to a request when you are charging a fee, you should follow our UK GDPR right of access guidance – 'Can we charge a fee?'.

Example

An accused person repeatedly makes SARs for a file containing personal information about their arrest. You have given them the same file before, and you have not collected any more information since their initial request. The request is excessive, but you decide to respond to the request because you think

they may have lost the file.

You tell the person you are charging them a fee for this information, based on administration costs. Once you receive the fee, you provide the information within one calendar month.

Relevant provisions in Part 3 of the DPA 2018 – The Part 3 provisions for manifestly unfounded and excessive requests are listed in Chapter 3, section 53

External link

Personal data breaches

At a glance

- Part 3 of the DPA 2018 introduces a duty on all organisations to report certain types of personal data breach to the Information Commissioner. You must do this within **72 hours** of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place.

In brief

- What is a personal data breach?
- What breaches do we need to notify the ICO about?
- What information must a breach notification to the Information Commissioner contain?
- When do we have to tell individuals about a breach?
- What information should we tell individuals who have been affected by the breach?
- How do we notify a breach?
- What should we do to prepare for breach reporting?

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

What breaches do we need to notify the ICO?

You only have to notify the ICO of a breach if it is likely to result in a risk to the rights and freedoms of individuals. If left **unaddressed** such a breach is likely to have a significant detrimental effect on individuals. For example:

- result in discrimination;
- damage to reputation;
- financial loss; or
- loss of confidentiality or any other significant economic or social disadvantage.

In more serious cases, for example those involving victims and witnesses, a personal data breach may cause more significant detrimental effects on individuals.

You have to assess this on a case by case basis and you need to be able to justify your decision to report a breach to the Information Commissioner.

What information must a breach notification to the Information Commissioner contain?

You must include:

- a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned;
  - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if you have one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures you have taken, or propose to take, to deal with the personal data breach and, where appropriate, of the measures you have taken to mitigate any possible adverse effects.

When do we have to tell individuals about a breach?

If a breach is likely to result in a **high risk** to the rights and freedoms of individuals, you must inform those concerned directly without undue delay.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO.

The duty to tell an individual about a breach does not apply if:

- you have implemented appropriate technical and organisational measures which were applied to the personal data affected by the breach (for example the data has been securely encrypted);
- you have taken subsequent measures which will ensure that any high risk to the rights and freedoms to individuals is no longer likely to materialise; or
- it would involve disproportionate effort.

Where a communication of a breach would involve disproportionate effort, you must make the information available to individuals in another, equally effective way, such as a public communication.

You may restrict the information, either wholly or partly, that you provide to individuals affected by a breach under certain circumstances. This is when doing so is a necessary and proportionate measure:

- to avoid obstructing an official or legal inquiry, investigation or procedure;

- to avoid prejudicing the prevention, detection, investigation or to prosecution of criminal offences or the execution of criminal penalties;
- to protect public security;
- to protect national security; or
- to protect the rights and freedoms of others.

What information should we tell individuals who have been affected by the breach?

You must give individuals information including:

- a description of the nature of the personal data breach;
- the name and contact details of the data protection officer (if relevant) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures you have taken, or propose to take, to deal with the personal data breach and, where appropriate, of the measures you have taken to mitigate any possible adverse effects.

How do we notify a breach?

You have to report a notifiable breach to the ICO without undue delay and within 72 hours of when you became aware of it. Part 3 of the DPA 2018 recognises that it will often be impossible for you to investigate a breach fully within that time-period and allows you to provide information in phases. If you cannot provide all the information required above within 72 hours, you must also explain reasons for the delay in your breach notification.

If the breach is sufficiently serious to warrant notification to the public, you must do so without undue delay.

Failing to notify a breach when required to do so can result in a significant fine up to £8.7m or 2 per cent of your global turnover.

To notify the ICO of a personal data breach, please see our pages on reporting a breach.

What should we do to prepare for breach reporting?

You should make sure that your staff understand what constitutes a personal data breach, and that this is more than a loss of personal data.

You should ensure that you have an internal breach reporting procedure in place. This will help decision-making about whether you need to notify the Information Commissioner or the affected individuals.

In light of the tight timescales for reporting a breach, it is important to have robust breach detection, containment, management and mitigation policies and procedures in place.

Relevant provisions of the DPA 2018 - See Sections 67, 68, Chapter 4

External link

National security provisions

At a glance

- Under Part 3 of the DPA 2018 individuals have rights of access, rectification, erasure or restriction, and to not be subject to automated decision-making.
- Some of these rights may be limited or restricted where this is a necessary and proportionate measure to protect national security. For ease of reference, these restrictions are referred to in this guidance as the national security provisions.
- The national security provisions may also limit your obligation to inform individuals about personal data breaches, where this is necessary and proportionate to protect national security.
- The national security provisions do not apply in a blanket manner. You must be able to show that deviating from specified data protection standards is necessary and proportionate to safeguard national security.
- A Minister of the Crown (specifically a member of the Cabinet, the Attorney General or the Advocate General for Scotland) can issue a certificate relating to the national security provision you wish to apply. You may rely on the certificate as conclusive evidence that the provision is a necessary and proportionate measure to protect national security. You should not assume that you must apply the provision, simply because a certificate has been issued. We publish details of relevant certificates.
- There is no exemption from, or restriction to, the data protection principles. You must always ensure your processing is generally fair and lawful, and complies with the other data protection principles.
- You must always comply with your general accountability and governance obligations.

Checklist for using the national security provisions

☐ We are a competent authority processing for law enforcement purposes.

☐ Our processing is fair and lawful, and we comply with the data protection principles.

☐ We comply with the data protection rights and obligations wherever possible, unless a restriction or limitation is necessary and proportionate to protect national security.

☐ We have considered the rights and legitimate interests of the individual, and have concluded that applying the national security provisions are a necessary and proportionate measure in the circumstances.

☐ We can point to a link between giving full effect to individuals' rights, or fully complying with our personal data breach obligations, and a potential adverse effect on national security.

☐ We have considered whether a national security certificate is applicable in the circumstances.

☐ We do not apply the national security provisions in a blanket manner, but only to the extent required to protect national security.

☐ We have considered whether we can inform the individual of the use of the provision, or whether this would itself undermine national security.

☐ We have recorded the use of the provision and can demonstrate its necessity and proportionality in light of the individual's rights and legitimate interests.

In brief

- Does this guidance apply to us?
- What are the national security provisions?
- What does national security cover?
- What are the effects of the national security provisions?
- When are the national security provisions likely to apply?
- What should we do if we restrict individuals' rights?
- What is a ministerial certificate?

Does this guidance apply to us?

This guidance applies to you if you are a competent authority processing for law enforcement purposes related to national security.

The rules governing law enforcement processing are set out in Part 3 of the DPA 2018.

If you are a competent authority processing data for a non-law enforcement purpose (eg for national security purposes only), the UK GDPR will apply to this processing. You should refer to our Guide to the UK GDPR.

If you are not a competent authority, and are processing personal data under the UK GDPR, different provisions apply. You should read our Guide to the UK GDPR.

The intelligence services themselves (or processors acting on their behalf) are covered by a separate regime. For more information, see our Guide to Intelligence Services Processing.

Further reading – ICO guidance

About the DPA 2018

What are the national security provisions?

The rights that individuals have when their data is being processed for law enforcement purposes are set out in sections 44 to 49 of the DPA 2018.

Some of these rights may be limited or restricted in certain circumstances. These circumstances are laid out in the provisions which set out the right. One of these circumstances is when restricting the right is necessary and proportionate to protect national security.

Section 68 sets out your obligations as a controller to inform individuals of a personal data breach which would be likely to result in a risk to their rights and freedoms. This obligation can be limited under certain circumstances. One of these circumstances is when limiting the information you provide is necessary and proportionate to protect national security.

For ease of reference, these restrictions and limitations are referred to in this guidance as the national security provisions.

You must still comply with the data protection principles, and with your accountability and governance obligations.

> Key provisions in the DPA 2018 - see sections 45; 46; 47; 48; 51; 68; 79
> External link

Further reading – ICO guidance

Principles
Accountability and governance

What does national security cover?

National security is not specifically defined and can be interpreted in a flexible way to adapt to changing threats. Thirty years ago, it would have been difficult or even impossible to predict the threats that developments in computer and communications technology could give rise to, or how such developments could be exploited by terrorists or hostile states. It is generally understood to cover the security and well-being of the UK as a whole, its population, and its institutions and system of government. For example, it can cover:

- protection against specific threats, such as from terrorists or hostile states;
- protection of potential targets even in the absence of specific threats; and
- international co-operation with other countries.

What are the effects of the national security provisions?

The provisions may permit you to restrict some of the data protection rights of individuals. The effects vary depending on the different rights. But in each instance, you can only apply the provision where this is a necessary and proportionate measure to protect national security.

Under the right to be informed, individuals have the right to be given privacy information about the collection and use of their personal data. You may be able to withhold some of this information, where this is necessary and proportionate to protect national security. Specifically, you may be able to withhold information about:

- the legal basis for processing;
- the length of time data will be retained for;
- the categories of any recipients of data; and
- any other further information you may normally provide to enable individuals to exercise their right of access.

You should provide as much of this information as you can, and only restrict the information where necessary and proportionate to protect national security.

Under the right of access, you may be able to withhold confirmation that you are processing personal data about a particular individual, and refuse to provide access to the data. Again, you should provide access to as much of the data as you can, and only withhold data where necessary and proportionate to protect national security.

Under the rights to rectification, erasure and the restriction of processing you would normally have to inform an individual exercising these rights whether you had refused their rights. However, you may be able to avoid informing them of this, to the extent that this is a necessary and proportionate measure to protect national security.

When dealing with a personal data breach, you would normally have to notify individuals who may be affected, if the breach is likely to result in a high risk to their rights and freedoms. However, you may be able to withhold this notification, where necessary and proportionate to protect national security.

When are the national security provisions likely to apply?

You can rely on the national security provisions to restrict individuals' rights or limit your personal data breach obligations, if you can show that doing so is a necessary and

proportionate measure to protect national security. This is linked to human rights standards, which mean that any interference with privacy rights must be necessary and proportionate in a democratic society to meet a pressing social need.

Although you are permitted to apply the national security provisions, where necessary and proportionate, you cannot do this in a blanket manner. Instead you need to consider applying the national security provisions on a case-by-case basis. In particular, it's not enough simply that the processing is related to national security. You must consider the actual consequences to national security if you had to provide the relevant information to the individual. If you can reasonably provide that information without affecting national security, you must do so (subject, of course, to any other restrictions that might apply in the specific circumstances).

When you consider whether to rely on a provision to withhold information, you must also consider whether you should withhold it "wholly or partly". In practice, this means that you must try and provide as much information to individuals as possible, and only withhold what is necessary to protect national security. So, if you can provide some information without posing any significant risk to national security, you must do so.

You don't need to show that providing the information would lead to a direct or immediate harm or threat. It is enough to show that there is a real possibility of an adverse effect on national security in a broader sense. For example, in freedom of information cases, courts have recognised that terrorists can be highly motivated. There may therefore be grounds for withholding seemingly harmless information on the basis that it may assist terrorists when pieced together with other information.

So, before withholding information you must first consider the fundamental rights and legitimate interests of the individual, and how these may be affected.

You must then consider whether withholding the information is a necessary and proportionate measure to protect national security. Keep in mind that there may be circumstances where the adverse effect on an individual could outweigh any trivial, or hypothetical risk to national security.

You must disclose it if, having considered this, you conclude that withholding the information is not necessary or proportionate.

If you decide to apply a national security provision, you should be able to make a reasoned and convincing argument about why this was necessary and proportionate. We may ask you for these arguments if we have received a complaint. You may base these on hypothetical scenarios, as long as they are realistic and credible.

For example, you may need to limit your response to a request under the right of access. You may apply a national security provision in order to provide a consistent "neither

confirm nor deny" (NCND) response about whether you process data for national security purposes. This may be necessary even in a case where there is no direct impact on national security, so that nothing can be inferred in other cases which might have more of an impact on national security.

You can apply this type of NCND response as a general policy. However, you should be able to make a reasoned argument about its use and demonstrate it to the ICO if required. You should still consider whether there are any special circumstances which mean you don't need to rely on the general NCND policy in a particular case.

The following example illustrates the process that a competent authority might go through to consider the application of the national security provisions. Although in practice you might consider the application of other restrictions first, this example shows how the process might work and how you may take NCND considerations into account.

Example

A police force receives a subject access request from an individual who is a subject of a covert counter-terrorism investigation. The police can apply a national security provision to restrict the individual's access to their personal data if this would risk harm to the investigation. For example by tipping off the individual about the investigation, or providing them with an opportunity to evade or frustrate the investigation.

Before applying the provision, the police need to consider whether the individual's rights or legitimate interests would be adversely affected. The individual's right of access would clearly be adversely affected. The police need to consider whether restricting the individual's right to access their personal data is a necessary and proportionate measure in light of the purpose for which they are restricting the rights, and the importance of the investigation in protecting national security.

The police do not have to inform the individual that their rights have been restricted, or the reasons for the restriction, if doing so would harm the investigation and pose a risk to national security. The police still need to inform the individual in general terms of their right to complain to the ICO or to apply to a court.

Once the investigation is complete, the police do not have to revisit the original subject access request, but if they receive a new request, they have to consider whether the restriction is still necessary. For example, to protect confidential sources, or other associated investigations. They also need to consider whether the restriction could be fully or partially removed.

Further reading – ICO guidance

The courts have considered a very similar exemption in the context of freedom of information requests. For more information, see our guidance on the FOI exemption for safeguarding national security.

What should we do if we restrict individuals' rights?

If you have restricted an individual's rights, you should normally inform them about:

- the restriction and the reasons for the restriction;
- their right to ask the ICO to check the restriction is lawful; and
- their right to bring a complaint to the ICO or apply to a court.

However, you may not have to inform individuals about the restriction and the reasons for it, if providing this information would itself undermine the purpose of the restriction.

Instead, you may consider issuing a more non-committal response. However, you should still provide anything which does not undermine the restriction. Wherever possible, also provide them with some information about their rights, in general terms. So, if you have refused to comply with an individual's request, you must still tell them about their right to complain to the ICO, or to apply to a court.

Individuals have the right to ask the ICO to check that any such refusal or restriction was lawful. This does not mean that the individual is able to circumvent the restriction and exercise their rights through the ICO instead. In many cases, we may be unable to be very specific about our findings because that might in itself reveal information which would prejudice the purposes the exemptions are designed to protect.

You need to record the restriction, and your reasons for applying it, so that you can show the ICO your reasons, if requested. You need to be able to show that you have applied the restriction only as far as necessary. Remember that you can apply the restriction wholly or partly to the right, and you should avoid applying it wholly unless that is necessary for protecting national security.

What is a ministerial certificate?

Section 79 of the DPA says that certain Ministers of the Crown (specifically, a member of the Cabinet, the Attorney General or the Advocate General for Scotland) can sign a certificate which is conclusive evidence that the restriction is a necessary and proportionate measure to protect national security.

It is important to remember that a certificate is not required in order for you to rely on the national security provisions. In fact in most cases, you will determine for yourself whether a restriction or limitation is required to safeguard national security (ie the application of a national security provision).

The provisions and the ministerial certificate do different things. The provisions, as detailed above, are always available and you may properly apply them to safeguard national security, with or without a ministerial certificate. Ministerial certificates are meant to give greater legal certainty that national security is applicable for specified data processing. This is because certificates certify that a restriction is a necessary and proportionate measure to protect national security.

In this context, a ministerial certificate is admissible as conclusive evidence that a restriction of an individual's rights or a limitation on a controller's obligations is necessary to protect national security.

These certificates can apply in advance, or they can be issued retrospectively for a restriction applied by a competent authority. The ICO publishes some details of all national security certificates which have been issued, including the text of the certificate where possible. However, there may be some cases where the text of the certificate is sensitive and cannot be published. In these cases, we publish the fact that a certificate was issued, the date it was signed, and which minister signed it.

If a relevant certificate is in place, you can rely on it to demonstrate that the restriction is necessary and proportionate. However, you should always consider whether you need to apply a restriction, or rely on any associated certificate, in a particular case. Individuals may challenge inappropriate reliance on a ministerial certificate in the Tribunal.

If you consider that a certificate is required, you can apply to a Minister of the Crown to issue a national security certificate under section 79. Details of the process for doing this are on the Home Office website, and linked to from the National Security Certificate page of the ICO website.

Individuals directly affected by a certificate can appeal against it to the Upper Tribunal. The certificate may be quashed if the Tribunal considers that the Minister did not have reasonable grounds for issuing it.

Individuals may also appeal to the Tribunal on the basis that the restriction the competent authority is relying on does not fall within the general description in the certificate.

For more information on ministerial certificates, see the Guide to Intelligence Services Processing.

Penalties

At a glance

- The Information Commissioner can issue a monetary penalty for failing to comply with Part 3 of the Act.
- There are two tiers of penalty – the higher maximum and the standard maximum.

In brief

- What penalties can the Information Commissioner issue?
- What is the higher maximum?
- What is the standard maximum?

What penalties can the Information Commissioner issue?

The Information Commissioner has the power to issue a monetary penalty for an infringement of the provisions of Part 3 of the Act – Law Enforcement Processing. Any penalty that we issue is intended to be effective, proportionate and dissuasive, and will be decided on a case by case basis.

Under Part 6 of the Act, there are two tiers of penalty for an infringement of Part 3 - the higher maximum and the standard maximum.

What is the higher maximum?

The higher maximum amount, is £17.5 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

In practice, the higher maximum amount can apply to any failure to comply with any of the data protection principles, any rights an individual may have under Part 3 or in relation to any transfers of data to third countries.

What is the standard maximum?

If there is an infringement of other provisions, such as administrative requirements of the legislation, the standard maximum amount will apply, which is £8.7 million or 2% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

> Relevant provisions of the Act - See Sections 155 to 159, Part 6
> External link

International transfers

Latest updates - last updated 09 March 2023

> **09 March 2023** - We have provided clarification about what, in our view, "strictly necessary" means for law enforcement international transfers. This imposes a more exacting standard than 'necessary', and in practice calls for a more rigorous justification for why you are processing and transferring the information. This update can be found under point one of the "Can we make a transfer to recipients other than relevant authorities?" section.

At a glance

- Part 3, Chapter 5 deals with when you can transfer personal data to a **third country**.
- A third country is a country or territory outside the UK.
- The DPA 2018 places limits on the circumstances when you can share.
- You have to meet certain conditions, including that the transfer is for one of the law enforcement purposes.
- Mostly, you can transfer to a **'relevant authority'** - a body entrusted with similar law enforcement responsibilities in the third country.
- There are specific provisions if you transfer to bodies that are not relevant authorities, with additional requirements which you must meet before you can do this.

Checklists

☐ We have checked whether we are a competent authority as defined by Schedule 7 of the DPA 2018.

☐ We have checked that the recipient is a relevant authority.

☐ We have confirmed whether the data was received from another competent authority.

☐ The transfer is necessary for one of the law enforcement purposes.

☐ The transfer is covered by adequacy regulations.

☐ If not, we are satisfied that the data will be subject to appropriate safeguards once transferred, and have notified the ICO about the categories of transfer we make on this basis.

☐ We are satisfied that the data will be subject to appropriate safeguards once transferred, and have notified the ICO about the categories of transfer we make on this basis.

☐ If not, we have identified special circumstances which still require the data to be transferred.

☐ We have taken steps to ensure that the data will not be further transferred elsewhere, and we have ensured that appropriate safeguards and conditions for any such onward transfer are in place, including limits on the extent of these transfers.

☐ If the transfer is to a recipient who is not a relevant authority, we have checked it meets the additional conditions, and we have notified the ICO.

☐ We have documented the transfer.

In brief

- What are the general principles for the transfer of personal data?
- Is the transfer covered by an adequacy decision?
- Can we make a transfer subject to appropriate safeguards?
- Are there any special circumstances?
- Can we make a transfer to recipients other than relevant authorities?
- What happens to subsequent transfers?

What are the general principles for the transfer of personal data?

There are three conditions that you have to meet before you can make a transfer:

- The transfer has to be necessary for any of the law enforcement purposes.
- The transfer has to be based on either a finding of adequacy in respect of the third country, or where other appropriate safeguards are in place, or if not, that the transfer is for certain specified special circumstances.
- The transfer is to a relevant authority in the third country, or is a 'relevant international organisation' ie an international body that carries out functions for any of the law enforcement purposes.

However it is still possible to transfer personal data to a body which is not a relevant authority, if you meet certain additional safeguards. See Can we make a transfer to recipients other than relevant authorities?

If the data is obtained from a competent authority in another EU member State, then that competent authority has to authorise the transfer. Except if:

- there is an immediate and serious threat to the public security of a third country; or
- there is an immediate and serious threat to the essential interests of an EU member State; and
- authorisation cannot be obtained in good time.

In such cases you must inform the relevant competent authority which would have been responsible for authorising the transfer without delay.

Is the transfer covered by an adequacy decision?

You may transfer personal data if the transfer is covered by UK adequacy regulations.

Adequacy regulations confirm that a particular third country (or a specified territory or sector in a third country) or international organisation has an adequate data protection regime to protect personal data. This is sometimes referred to as an 'adequacy decision'.

There are adequacy regulations in place to cover transfers to:

- EEA States. (The EU member states and Iceland, Liechtenstein and Norway);
- Gibraltar;
- Guernsey;
- Jersey; and
- Switzerland.

The ICO's role in assisting the Home Office with this work is set out in a Memorandum of Understanding between the two authorities. Any future adequacy regulations will be finalised in accordance with this Memorandum and issued by the UK Government.

Can we make a transfer subject to appropriate safeguards?

If there is no 'adequacy decision' about the country, territory or sector for your restricted transfer, you may still make the transfer on the basis that other appropriate safeguards exist to ensure that individuals' rights are enforceable and effective legal remedies are available following the transfer.

Appropriate safeguards may be provided for by:

- a legal instrument providing appropriate safeguards which binds the intended recipient; or
- an assessment performed by the controller which concludes that appropriate safeguards exist. In this case, you must inform the Information Commissioner of the

categories of data transfers that take place.

You must document the transfer, and provide this documentation to the Information Commissioner on request. You must record:

- the date and time of the transfer;
- the name, and any other pertinent information about the recipient;
- the justification for the transfer; and
- a description of the data you transferred.

You must ensure that any personal data you have transferred is not further transferred to another third country without your authorisation, or authorisation from another UK competent authority, and any authorisation can only be given where the transfer is necessary for any of the law enforcement purposes.

Are there any special circumstances?

Sometimes, you may need to transfer personal data when there is neither a finding of adequacy, nor appropriate safeguards in place. This can only take place in certain, specified circumstances, referred to as the 'special circumstances'. These are listed in the DPA 2018 as the five circumstances where the transfer is necessary:

1. To protect the vital interests of the data subject or another person;
2. To safeguard the legitimate interests of the data subject;
3. For the prevention of an immediate and serious threat to the public security of third country;
4. In individual cases for any of the law enforcement purposes; or
5. In individual cases for a legal purpose.

There are a few things to keep in mind.

You need to document the transfer, and provide those records to the Information Commissioner on request. You must record:

- the date and time of the transfer;
- the name, and any other pertinent information about the recipient;
- the justification for the transfer; and
- a description of the personal data you transferred.

These are the same details that you are required to record for transfers on the basis of appropriate safeguards.

Items 4 and 5 of the special circumstances provide for a degree of flexibility, but in those cases it is necessary for you to specifically consider the rights and freedoms of the individual whose data you are transferring. If those rights and freedoms override any public interest in the transfer, then the transfer cannot take place on the basis of special circumstances. Items 4 and 5 are case-specific and this safeguard is there to make sure that the individual's interests remain at the heart of matters. In such cases, if the transfer is still necessary, you will need to apply another lawful basis for the transfer.

A transfer is deemed to be necessary under item 5:

- for the purpose of, or in connection with, any legal proceedings for any of the law enforcement purposes. This can include prospective legal proceedings, ie where the proceedings are anticipated, but have not yet commenced;
- for the purpose of obtaining legal advice in relation to any of the law enforcement purposes; or
- for the purpose of establishing, exercising or defending legal rights in relation to any of the law enforcement purposes.

In each case, the circumstances must link directly back to any of the law enforcement purposes to which Part 3 of the Act relates.

Can we make a transfer to recipients other than relevant authorities?

For the most part, it is expected that transfers will take place between 'relevant authorities', or relevant international organisations ie to any (legal) person in the third country (or operating internationally) who has functions comparable to those of a 'competent authority' for the purposes of Part 3 of the DPA 2018.

Sometimes, however, you may need to transfer personal data to a recipient that is not a relevant authority. Before you can do this, you must meet all four of these additional conditions:

1. The transfer is strictly necessary in a specific case, for the performance of a task by the transferring controller, as provided by law for any of the law enforcement purposes.

   In item 1, 'strictly necessary', as required in some sections of Part 3 DPA 2018, imposes a more exacting standard than 'necessary', and in practice calls for a more rigorous justification for why you are processing the information.

   Further, the transfer must be for the performance of a task for which you have a lawful

purpose under the law enforcement provisions of Part 3 of the DPA 2018.

2. The fundamental rights and freedoms of the data subject do not override the public interest concerning the transfer.

   Item 2 means that the rights and freedoms of the data subject can override any public interest in the transfer, so if the rights and freedoms of the data subject in not having their data transferred to the intended recipient are of equal or greater importance than the public interest in transferring the data, then the transfer shall not take place.

3. The transferring controller considers that the transfer to a relevant authority in the third country would be ineffective, or inappropriate.

   Item 3 means that, where possible, transfers to a third country should be undertaken to a relevant authority in that country, and it is only in circumstances where transferring the data to such a relevant authority would be ineffective or inappropriate, that a transfer to another recipient should be contemplated. Transfers may be ineffective, for example, if the transfer is time-critical and the relevant authority would be unable to act on the transfer in sufficient time. A transfer may be inappropriate if the transfer to the relevant authority might prejudice the purposes of the transfer, for example if the data relate to allegations of corruption or impropriety in the relevant authority and there is a risk that the transfer may tip-off relevant personnel within that authority that an investigation is underway.

   Where you have transferred data to a body other than a relevant authority, you must inform the relevant authority in that country of the transfer, unless, as above, that would be ineffective or inappropriate.

4. The transferring controller sets out the specific purposes for which the data may be processed by the intended recipient and informs them of these.

   You need to document the transfer, and you also need to notify the Information Commissioner about the transfer. This is different to other types of transfers, where you record the details but only have to provide them to the Commissioner on request.

What happens to subsequent transfers?

It is important that control of personal data is not lost once you have transferred it. It is vital that the rights and freedoms of individuals are still uppermost. Therefore, if the data you transferred is to be subsequently transferred elsewhere, it is important that those rights and freedoms continue to follow the data. For this reason, there are certain provisions that you must observe before any subsequent transfer can take place.

Firstly, you must make it a condition of the transfer that any subsequent transfer must be authorised by you, or another competent authority. It would be sensible to have

agreements in place with any other competent authorities who you may consider allowing to make such an authorisation.

Secondly, any authorisation can only be for a transfer which is necessary for any of the law enforcement purposes, and you must give consideration to:

- the seriousness of the circumstances leading to the request for authorisation of the subsequent transfer;
- the purpose for which you originally transferred the data; and
- the standards of data protection which apply in the country or international organisation where the data will be transferred.

If you originally received the data from a competent authority in an EU member state, that competent authority must first authorise the transfer before you in turn can authorise it. This creates a chain of accountability, linking back to the original competent authority which first held the data, which ensures that the original competent authority retains a measure of control and influence over any processing of that data.

The only exception is if the transfer is necessary for the prevention of an immediate and serious threat to the public security of a third country, or to the essential interests of an EU member state (note, not the essential interests of any third country) and you cannot obtain authorisation from the originating competent authority in good time. If that happens, then you should inform the originating competent authority without delay.

Relevant provisions of the legislation - see DPA 2018 sections 72 to 78, Chapter 5

External link

Resources

This page contains resources and support that organisations in the police, justice and surveillance sector may find useful.

Appropriate policy document

Part 3 - appropriate policy document

For organisations
Word (74.6KB)

Paying the data protection fee

On 1 April 2019, the rules around paying the data protection fee changed. Members of the House of Lords, elected representatives and prospective representatives **(including police and crime commissioners)** are exempt from paying a fee, unless they process personal data for purposes other than the exercise of their functions as a Member of the House of Lords, an elected representative or as a prospective representative. For more information, read our guidance on the data protection fee.

The use of live facial recognition technology by law enforcement in public places

The Information Commissioner has issued the first Commissioner's Opinion under data protection law about the use of live facial recognition technology be law enforcement.

Commissioner's opinion

External link

Processing gangs information: a checklist for police forces

The ICO recently issued an Enforcement Notice to the Metropolitan Police Service (MPS) in relation to their Gangs Matrix, after we found it breached data protection laws. You can read a blog about it. The ICO is also investigating how information about gangs is used by other public authorities.

This checklist has been created specifically for police forces who might be using, or considering using, a Gangs Matrix, or similar system. Please note that the checklist will help you to assess compliance with data protection law, and is a guide – not a guarantee of compliance.

Surveillance

Our team often receives enquiries about surveillance technology including body worn video, ANPR and unmanned aerial systems. Advice about these technologies is provided in the updated version of the CCTV code of practice. The code sets out the Information Commissioner's recommendations on how organisations can process personal data within the legal requirements of the Data Protection Act when using these technologies.

Toolkit for organisations considering using data analytics

A toolkit designed to help the law enforcement sector comply with data protection law when using data analytics has been created by the ICO. The toolkit will be most helpful to you if your organisation is at the beginning of your data analytics project lifecycle. It will help you to recognise some of the central risks to the rights and freedoms of individuals created by the use of data analytics.

The Home Office has published detailed guidance for police forces about the use of body worn video (BWV), which takes into account the management of personal data obtained by the cameras.

> ### Home Office guidance - Safeguarding body worn video data
> External link

> ### Home Office guidance - Technical guidance for body worn video devices
> External link

Guidance about data protection concerns and BWV was also produced by The College of Policing in August 2014.

> ### College of Policing guidance - Body Worn Video
> External link

You may also be interested in reading our guide on the responsible recreational use of drones – also called unmanned aerial systems (UAS) or unmanned aerial vehicles (UAVs).

We liaise with the Surveillance Camera Commissioner where appropriate. The Surveillance Camera Commissioner has also produced a code of practice.

> ### Surveillance camera code of practice
> External link

There is more information available about the role of the Surveillance Camera Commissioner and the tools available to help with compliance.

Surveillance Camera Commissioner

External link

Security

Data Controllers must ensure that they take appropriate technical and organisational measures against unlawful or unauthorised processing, accidental loss, destruction or damage to personal data. Some of the ICO's largest civil monetary penalties have been served on data controllers in the police, justice and borders sectors. This frequently occurs where insufficient safeguards have been in place for handling sensitive personal data. Here you will find advice on security measures safeguarding cloud computing and privacy impact assessments.

ICO training video: Data Protection Act 2018 (Part 3)

This ICO training module is relevant for controllers and processors who process personal data in connection with law enforcement. They explain the purposes for using personal data in this way and when people's rights relating to their data may be restricted.

Module 12(a): Data Protection Act 2018 (Part 3)

Video opens in Vimeo

Data Protection and PECR Training Supporting notes and further reading Module 12: DPA Part 3

For organisations
PDF (235.6KB)

Further reading

The Right of Access – Part 3 of the DPA 2018

Latest updates - last updated 10 February 2023

> **10 February 2023** - This guidance was published.

This guidance discusses the right of access to information processed for a law enforcement purpose under Part 3 of the Data Protection Act 2018 (DPA 2018) in detail. Read it if you have detailed questions not answered in the Guide, or if you need a deeper understanding to help you apply the right of access under Part 3 in practice. It is aimed at 'competent authorities' who process personal information for any of the law enforcement purposes. In particular, Data Protection Officers (DPOs) and those with specific data protection responsibilities in the context of law enforcement processing.

If you haven't yet read the 'in brief' page on the Part 3 right of access, you should read that first. It introduces this topic and sets out the key points you need to know, along with practical checklists to help you comply.

You should read this guidance if you have specific questions about dealing with subject access requests (SARs) in the context of law enforcement processing. You might also find it helpful to refer to the detailed UK GDPR guidance on the right of access and we will signpost to this guidance when it may be useful.

You should also read the separate law enforcement guidance on manifestly unfounded and excessive requests.

Where your processing operations are for general purposes only, you should refer to the right of access guidance under the UK GDPR.

To help you understand the law and good practice as clearly as possible, this guidance says what organisations **must**, **should**, and **could** do to comply.

Legislative requirements

Must refers to legislative requirements.

Good practice

Should does not refer to a legislative requirement, but what we expect you to do to comply effectively with the law. You should do this unless there is a good reason not to. If you choose to take a different approach, you must be able to demonstrate that this approach also complies with the law.

Could refers to an option or example that you could consider to help you to comply effectively. There are likely to be various other ways you could comply.

Further reading – responses to the ICO's consultation

In December 2021, we launched a public consultation on the detailed guidance on the Part 3 right of access, and on the updated guidance on manifestly unfounded and excessive requests. You can read a summary of responses to the consultation and the ICO's comments here.

Contents

What is the right of access in Part 3 of the DPA 2018?

- What is the right of access in the context of law enforcement processing?
- What does “safeguarding against and the prevention of threats to public security” mean?
- What information is someone entitled to under Part 3?
- What other information is someone entitled to under Part 3?
- Are people only entitled to their own personal data?
- Who is responsible for responding to a request?
- When do we need to take action to enable someone to make a SAR?

How do we recognise a Part 3 subject access request (SAR)?

- What is a Part 3 subject access request (SAR)?
- Are there any formal requirements?
- Do we have to respond to the SAR if the person has an alternative means of accessing their information?
- Can someone ask a third party to make a SAR on their behalf?
- How do we decide which SARs regime applies?
- What is the primary purpose for processing?
- What happens if our primary purpose for processing changes, or if the information we collect is no longer relevant?
- At what point do we decide which SARs regime applies?
- Do we need to provide information processed for logging purposes?
- How do we deal with requests for unstructured manual records?

What should we consider when responding to a Part 3 request?

- How long do we have to comply?
- Can we extend the time for a response?
- If both the UK GDPR and Part 3 information is covered by the SAR, can we deem the request complex and extend the deadline?
- How long do we have to deal with requests for information processed for different purposes?
- Can we clarify the request in Part 3?
- Can we stop the clock and ask for clarification?
- Can we charge a fee under Part 3?

How should we supply Part 3 information to the requester?

- What information must we supply under Part 3?
- In what format should we provide the information?
- What should we do if the information exists in different forms?
- Can we provide remote access?
- In what circumstances can we provide someone with access to their information but not a copy?
- Do we need to make reasonable adjustments for disabled people?

Can we restrict the right of access under Part 3?

- Can we restrict access to the information we provide under Part 3?
- What is a 'necessary and proportionate measure'?
- What rights and interests may be impacted by restricting someone's right of access?
- When can we neither confirm nor deny we hold the information?
- What does "avoid obstructing an inquiry, investigation or procedure" cover?
- What does "avoid prejudicing" cover?
- What does "protect public security" cover?
- What does "protect national security" cover?
- What does "protect the rights and freedoms of others" cover?
- Can we restrict the right of access for more than one reason?
- Can we restrict the right of access for a specified period of time?
- Do we need to record our reasons for restricting someone's right of access?
- Do we need to tell people why their rights have been restricted?
- Can we rely on the UK GDPR exemptions to withhold personal information under Part 3?
- Can we withhold information on the basis of 'legal professional privilege'?

What should we consider when acting as joint controllers?

- What do we need to consider if we are acting as joint controllers?
- What are the responsibilities of the "contact point"?
- Do we need to consult with joint controllers before responding to a SAR?
- What happens if we are only processing some of the requested information for joint purposes?
- Can we consult other competent authorities when deciding whether to apply a restriction?
- What happens if independent controllers are processing the same information for different purposes?

What should we do if the Part 3 request involves information about other people?

- What is the basic rule?
- What approach should we take?
- What about confidentiality?
- Does categorising people impact what information we can provide them with?
- How should we deal with requests from people who fall within multiple categories?

What do we need to consider if personal information is processed by a court for law enforcement purposes?

- Does someone have a right to access personal information created by a court?
- What does "by or on behalf of a court or other judicial authority" mean?
- What is a "judicial decision"?
- What information will be created by or behalf of a court for a criminal investigation?
- What information will be created by or on behalf of a court for criminal proceedings?
- What does "relating to" mean?
- What does "for the purpose of executing a criminal penalty" mean?
- Does the exception cover documents filed or placed in the custody of the court?
- Does the exception apply if the court has shared the information with another organisation?
- Is this exception time-bound?

Can the right of access be enforced under Part 3?

- What enforcement powers does the ICO have?
- Can a court order be used to enforce a SAR?
- Can people be awarded compensation?
- Is it a criminal offence to destroy and conceal information?

What is the right of access in Part 3 of the DPA 2018?

In detail

- What is the right of access in the context of law enforcement processing?
- What does "safeguarding against and the prevention of threats to public security" mean?
- What information is someone entitled to under Part 3?
- What other information is someone entitled to under Part 3?
- Are people only entitled to their own personal information?
- Who is responsible for responding to a request?
- When do we need to take action to enable someone to make a SAR?

What is the right of access in the context of law enforcement processing?

Section 45(1) of the DPA 2018 gives people a right to obtain their personal information that is being used for a law enforcement purpose.

This right allows people to request a copy of their personal information from you, as well as other supplementary information. These requests are usually called subject access requests (SARs).

The right of access helps people understand how and why you are using their information and check you are doing so lawfully. You **must** publicise the right of access, for example, on your website, in your privacy statement, or in other communications with people.

You **must** only use Part 3 for responding to SARs, if you are:

- a competent authority; and
- using the information for one of the law enforcement purposes.

The law enforcement purposes are defined under section 31 as,

> "…the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".

What does "safeguarding against and the prevention of threats to public security mean?"

This means preventing and safeguarding against threats to public security, where this fits broadly within the wider law enforcement purposes of:

- preventing, investigating, detecting or prosecuting crime, or
- executing criminal penalties.

For example, safeguarding against threats to public security may apply to covert surveillance or video surveillance for the prevention and detection of crime. You **should** consider these uses of personal information under Part 3.

It does not mean wider public security threats, such as natural disasters or other major incidents, that are not usually linked to criminal offences or penalties. You **should** consider your uses of personal information for these wider threats under the UK GDPR.

What information is someone entitled to under Part 3?

The right of access under Part 3 gives people the right to obtain the following from you:

- confirmation that you are using their personal information;
- access to their personal information; and
- other supplementary information.

Where possible you **must** respond in writing and provide the person with a copy of their information – unless you don't hold the information, or you believe a restriction applies. You **could** provide the information in its existing format, if this is the most accessible form. For example, where you cannot convey the full context and meaning of the information solely in writing. This may include providing secure access to CCTV footage, or audio recordings. You do not have to create transcripts to respond to a request, if you do not already have them.

In most cases, you can confirm whether you are using a person's personal information in general terms. However, if the request is for a specific piece of information, you **should** generally be able to confirm or deny whether you are processing the information unless a restriction applies. Depending on the circumstances, and due to the sensitivities of law enforcement processing, you may not be able to be fully transparent with the person about the nature of the processing or whether you hold the information (see When can we neither confirm nor deny we hold the information?).

You **must** ensure that your processing is lawful and fair, and aim to be as open and transparent as possible with people about how you use their personal information.

However, in some circumstances transparency can undermine your law enforcement activities, and you may be unable to confirm or deny whether you are processing personal information. However, you may only restrict a person's right of access, if one of the

restrictions listed in section 45(4) applies.

What other information is someone entitled to under Part 3?

People have the right to receive the following information (which largely corresponds with the information that you should provide in a privacy notice):

- your purposes and lawful reason (known as lawful basis) for processing;
- categories of personal information you're processing;
- recipients or categories of recipient you have disclosed the personal information to (including recipients or categories of recipients in third countries or international organisations);
- your retention period for storing the personal information or, where this is not possible, the criteria for determining how long you will store it;
- the person's right to request rectification, erasure or restriction of the information you are processing;
- the person's right to lodge a complaint with the Information Commissioner's Office (ICO);
- details of the personal information you are processing; and
- any available information about the source of the information.

When responding to a SAR, you **must** supply this information in addition to a copy of the personal information itself, even if the person does not specifically ask for it. If you provide this information in your privacy notice, you **could** provide a link to it or a copy.

In using personal information for a law enforcement purpose, you **must** distinguish, where possible, between the different categories of people whose information you process. This may include information about a suspect, offender, complainant, victim, witness, informant, or any other person. How you categorise a person may affect:

- what information you are able to provide;
- how you search for information (eg if it is held in different contexts); or
- if you need to restrict a person's right of access to their information.

Are people only entitled to their own personal information?

Yes, in most circumstances, unless:

- their information also relates to other people; or
- they are exercising another person's right of access on their behalf.

Before you respond to a SAR, you **must** decide whether the information you hold is personal information and, if so, who it relates to.

For information to be personal information, it must relate to a living person who is identifiable from that information (directly or indirectly). In most cases, it is obvious whether the information is personal information, but we have produced guidance on What is personal data? to help you decide if it is unclear.

The same information may be the personal information of two (or more) people, and you may therefore be able to restrict the person's right of access. Please see What should we do if the Part 3 request involves information about other people? for further details.

Who is responsible for responding to a request?

This depends on whether you are a "controller" or a "processor". Controllers are responsible for complying with SARs, not processors.

If you use a processor, you **must** have contractual arrangements in place to guarantee that you can deal with SARs properly, whether they are sent to you or the processor. The processor **must** help you meet your obligations for SARs and you **must** make this clear in the agreement between you.

In most cases, the processor may hold personal information on your behalf. If so, you **should** be able to require the processor to search for this information and, if necessary, give you a copy. However, it is still your responsibility to decide how to deal with the request.

If you are a joint controller, you **must** have an arrangement in place with your fellow joint controller(s) that sets out each of your responsibilities, including how you deal with SARs. Under Part 3, you **must** specify a central point of contact for people, which **must** be one of the joint controllers. See What should we consider when acting as joint controllers?.

Further reading

UK GDPR guidance:

- Controllers and processors
- Contracts

When do we need to take action to enable someone to make a SAR?

People have a right to be informed about how you are using their personal information. Where possible, you **should** be open and transparent about what information you process about them, and why you are processing it. Letting people know that you are using their

personal information will greatly assist them in exercising their right of access under Part 3.

People may not always know that you hold information about them (or have enough information to be able to make a SAR), particularly if you have obtained it from another source. In these circumstances, you **must** provide the person with the following information, unless a restriction applies:

- your lawful basis for processing;
- your retention period for storing the personal information or, where this is not possible, the criteria for determining how long you will store it;
- if applicable, recipients or categories of recipient you have disclosed the personal information to (including recipients or categories of recipients in third countries or international organisations); and
- any other information the person needs to be able to make a SAR.

You **could** contact the person directly or direct them to the privacy information on your website.

You may withhold some of the information listed above, if a restriction applies (eg where complying with the SAR may prejudice a criminal investigation). Follow the approach outlined in the chapter Can we restrict the right of access under Part 3? In deciding whether to withhold some of the person's privacy information, you **must** consider how this might impact their rights and interests.

You **should** consider any decision on whether you can restrict the person's right to any of their privacy information on its own merits. You **should** treat this separately from any decision about whether you need to confirm the information is held, or apply a restriction to the person's right of access.

Example

The police are conducting a covert operation to investigate a serious crime. They obtain information about a person from various sources, including through using invasive technology, such as audio recording devices.

The police decide that restricting access to the person's privacy information is necessary to avoid prejudicing a criminal investigation. Therefore, the person is not aware that police are collecting and processing information about them.

However, once the investigation is complete, it is no longer necessary or proportionate to apply the restriction. The police should inform the person that they hold their information, and direct them to any relevant privacy information,

as appropriate. They cannot withhold this information just because it may be inconvenient to provide it. Although they may apply a further restriction, if necessary. It is important that the police document the reasons for their decision.

Relevant provisions in the legislation - See DPA 2018 Sections 43-45; 55-59; and 64-65

External link

Further reading – ICO guidance

- Which regime
- UK GDPR guidance on contracts between controllers and processors
- UK GDPR guidance on controllers and processors
- UK GDPR guidance on DPIAs
- Guide to Law Enforcement Processing
- Part 3 guidance on the right to be informed
- Part 3 guidance on categorisation
- Part 3 guidance on what is a 'competent authority'?

How do we recognise a Part 3 subject access request (SAR)

In detail

- What is a Part 3 subject access request (SAR)?
- Are there any formal requirements for how someone should make a SAR?
- Do we have to respond to the SAR if the person has an alternative means of accessing their information?
- Can someone ask a third party to make a SAR on their behalf?
- How do we decide which SARs regime applies?
- What is the primary purpose for processing?
- What happens if our primary purpose for processing changes, or if the information we collect is no longer relevant?
- At what point do we decide which SARs regime applies?
- Do we need to provide information processed for logging purposes?
- How do we deal with requests for unstructured manual records?

What is a Part 3 subject access request (SAR)?

A Part 3 SAR is a request made by or on behalf of someone for the information they are entitled to ask for under section 45(1). They may ask you to:

- confirm whether or not you are processing their information; and if so,
- provide them with access to it.

Are there any formal requirements for how someone should make a SAR?

No, Part 3 does not set out formal requirements for a valid request. Anyone can make a SAR verbally or in writing, including by social media. They can make it to any part of your organisation. They do not have to direct it to a specific person or contact point, tell you why they are making the request, or what they intend to do with the information.

A request does not have to include the phrases "subject access request", "right of access", or "section 45(1) of the DPA 2018". It just needs to be clear that the person is asking for their own personal information. Indeed, a request may be a valid SAR even if it refers to other legislation, such as the Freedom of Information Act 2000 or the Freedom of Information (Scotland) Act 2002.

In general, you **should** have a single contact point for SARs. If you are a joint controller, you **must** ensure that you designate a "contact point" for people who wish to make SARs. You **must** cover this in your joint controllership arrangements. See What should we

consider when acting as joint controllers?.

You **should** have a policy for recording details of all the requests you receive. You **should** keep a log of any verbal requests you receive, as these are also considered valid SARs.

Do we have to respond to the SAR if the person has an alternative means of accessing their information?

Yes. A SAR is still valid even if the person has the option of using another statutory disclosure or legal route to obtain their information. Examples of other routes include the Criminal Procedure and Investigations Act 1996, or the Criminal Justice and Licensing (Scotland) Act 2010.

They may not have received all of the personal information held about them through that alternative means, or only have had an opportunity to inspect their information, and may not have received a copy. You may also hold information about them that you were not required to disclose under the alternative route, or new information about them that did not exist when they obtained information through the alternative means.

If you are aware that someone is seeking their information for a specific purpose (eg for court proceedings), you **could** remind them that they will only be able to obtain their own personal information by making a SAR, and not information about other people.

You **could** explain to them what other routes may be available to them for obtaining their information, and in some circumstances, they may agree to use an alternative method instead. However, you **must not** refuse to comply with a SAR just because someone has an alternative means of accessing their personal information.

Example

A person who was injured in a road traffic collision makes a SAR to the police in order to pursue a civil claim for damages against the driver responsible for the accident.

The police are aware that the person will be able to obtain this information through other legal mechanisms once they bring a claim. In responding to the SAR, the police are aware they will need to redact the personal information of other people before disclosing it. As the information will be redacted, the police expect that it may have limited use as evidence at court.

The police contact the person and explain that they will need to redact some of the information, and as such, this might not be helpful if the person requires the information for legal proceedings. They also suggest that it would be a good idea

for the person to discuss the matter with their solicitor, as there may be other legal methods of obtaining the information they need. However, they also make it clear that the person is entitled to make a SAR for this information.

If the person still wants to make a SAR, the police should respond within one month of first receiving the request.

Alternative disclosure mechanisms may not involve direct disclosure to the person themselves, as the information may be provided to their lawyers. Lawyers are generally under an obligation to make their client aware of all material information in their possession. But this does not mean the person is able to access their information just because it has been made available to their lawyer through another process. You **should** carefully consider the circumstances of the request, particularly where someone may have changed their legal representative.

However, there may be limited circumstances when you can refuse to deal with a SAR because the person has an alternative way to access their information. In particular, if the person has already been given exactly the same information (as they have now requested) and you can demonstrate that their new request is part of a pattern of disruptive behaviour. For further details, see our guidance on manifestly unfounded and excessive requests.

Can someone ask a third party to make a SAR on their behalf?

Some people may prefer a third party to make a SAR on their behalf (eg a relative, friend or solicitor). In the context of criminal justice and law enforcement, it is not uncommon for people to ask their solicitor to act on their behalf. Part 3 does not prevent this. However you need to be satisfied that the third party making the request is entitled to act on behalf of the person. Follow the recommendations in our UK GDPR detailed right of access guidance Can an individual make a request on behalf of someone?.

If a third party makes a SAR on behalf of an someone else, you **should** respond to the requester as if you were responding directly to the person the information is about.

Example

A requester makes a SAR to the Planning Service on behalf of their mother, who is being prosecuted for failure to comply with an Enforcement Notice to remove an illegal house extension. The requester is appropriately authorised to act on their mother's behalf, and to obtain the information. The Planning Service is satisfied that it is appropriate to release the information to the requester.

However, the information contains some personal information of the requester, who is acting on behalf of their mother. The requester's personal information contains important context about the circumstances of the prosecution. However, the Planning Service must deal with the SAR as if it had been made by the person themselves. As it is releasing the information directly to the requester, it contacts them to enquire whether they are happy for their personal information to be disclosed in the response.

However, if the Planning Service sends the response directly to the mother, it should redact the personal information of the requester, as it would have done if the mother had made the SAR directly. If the Planning Service is unable to contact the requester to check their preference, it should be cautious and redact the requester's personal data.

In circumstances where someone has appointed a legal representative or other professional to act on their behalf, you may receive repeat requests for information that you have previously disclosed. For example, if the person changes their representative. How you respond may depend on the circumstances, and on any other laws or policies you are subject to. You **should** document the reasons for your decision.

Depending on the circumstances, you **could** also consider such requests to be manifestly unfounded or excessive. See our Guide to Law Enforcement processing – Manifestly unfounded or excessive requests.

Example

A solicitor makes a SAR to the prosecution service on behalf of someone who was convicted of assault occasioning actual bodily harm. The prosecution service discloses the information. Several weeks later, the person changes their solicitor, who then makes a request for the same information.

The prosecution service considers the SAR as if it had been made by the person themselves. It could therefore view the SAR as a repeat request, which means the manifestly excessive provisions may apply to the information which has already been disclosed. However, depending on the circumstances, the prosecution service may still decide to provide this information. For example, it may consider any relevant legislation, policies, or other matters, including any difficulties the person might have in obtaining the information, or the impact on them if it does not provide the information.

However, if it has obtained any new information since responding to the previous request, it should provide it unless a restriction applies. It is important that the prosecution service documents the reasons for its decision.

You may also receive requests for information made on behalf of someone through an online portal. See our UK GDPR detailed right of access guidance Do we have to respond to requests made via a third party online portal?.

If you receive requests by or on behalf of children or young people, see our UK GDPR detailed right of access guidance What about requests for information about children or young people?.

How do we decide which SARs regime applies?

Before responding to a SAR, you **must** determine whether you are using the personal information for general purposes or for any of the law enforcement purposes. This is important as there are many differences between the UK GDPR and Part 3. You may also process information for more than one reason.

If your primary purpose for using the information is for one of the law enforcement purposes, you **must** deal with the SAR under Part 3. If you are using the information for general purposes, you **must** deal with the SAR under the UK GDPR.

You **should** consider your reason for processing the information at the time you receive the request.

Example

A seaside town regularly experiences flooding. The police work with other agencies to develop an incident response plan, which explores how to prevent future floods, and how best to protect human life and property should future incidents occur.

While dealing with such emergencies is an important policing function, it is not criminal law enforcement. Any of the personal information police collect about this matter should therefore be processed under the UK GDPR. If police receive a SAR from someone whose information they process for this purpose, they should deal with it under the UK GDPR, not Part 3.

If you process the same personal information for more than one purpose (eg for a law enforcement purpose and for general purposes), you need to identify your **primary**

purpose for processing the information.

What is the 'primary purpose' for processing?

The term 'primary purpose' is not defined in the legislation but generally means your principal objective for processing the information. This does not necessarily mean your original reason for collecting it.

In general, any information you obtain in connection with your law enforcement purposes is likely to be processed under Part 3. This can include (but is not limited to):

- information you discover, seize, or download as part of an investigation;
- expert reports (eg medical or forensic);
- legal advice; or
- information provided to you by third parties.

Although your primary purpose for processing the information will usually be obvious, you **should** consider the following factors, if you aren't sure:

- your reasons for collecting or obtaining the information;
- any legislation that forms the basis of your processing, and whether it has an underlying law enforcement purpose;
- whether your purpose for processing has changed;
- any relevant policies; and
- any other relevant circumstances.

Example

A suspect is detained in a custody suite on suspicion of having committed an offence. They have a pre-existing medical condition that requires them to take medication at regular intervals.

The custody officer has been provided with some of their medical information to enable the suspect to self-administer their medication.

The suspect makes a SAR for all the information held about them.

While the information relating to the criminal offence will clearly be dealt with under Part 3, the organisation needs to decide whether their primary purpose for processing the medical information is under the UK GDPR, or Part 3. They may consider any relevant legislation or policies (eg about the care and welfare of detainees at police stations) or any other matter. They should also document the reasons for their decision.

Your reason for processing the information may change over time. You may collect information under the UK GDPR (eg for general administrative purposes), but as circumstances progress and the purpose changes (eg as you identify elements of criminality), you may end up processing it for law enforcement purposes (under Part 3) instead or under both simultaneously.

Example

Police process information about a disciplinary matter between two staff members during their employment. There is an ongoing dispute between them which has resulted in numerous arguments and allegations of harassment and bullying by both parties. The police are processing this information under the UK GDPR, and dealing with it in accordance with standard policies.

However, while investigating the matter, the police identify potential criminal issues. Following this, the investigation into the matter becomes a criminal investigation.

Both people make a SAR for the personal information held about them in relation to this matter. As it is now being treated as a criminal investigation, the police should deal with the SARs under Part 3.

It may be easier to identify a change in regime if the information is passed to a specialist team or department to use for a specific purpose. You may also have the option of dealing with a particular issue either as a criminal or civil matter.

Example

A dedicated fraud unit has obtained information about someone for the purposes of an investigation. It received this information from another department that had collected it under the UK GDPR, as part of its routine processing operations.

The fraud unit has powers to deal with the matter as a civil or criminal investigation. If it decides to deal with it as a criminal investigation, then it should use Part 3 to process the information. However, if it treats the matter as a civil investigation, the fraud unit will be processing the information under the UK GDPR instead.

Remember that you **should** document your rationale.

What happens if our primary purpose for processing changes, or the information we collect is no longer relevant?

If you originally collected the information under the UK GDPR, you will be able to use it for law enforcement purposes under Part 3, if it becomes relevant to a criminal matter. If you receive a SAR, you **should** carefully consider your main reason for processing the information.

> **Example**
>
> The police receive a SAR from a staff member for details of their medical absences within the last three years. Their human resources file contains information relevant to a criminal investigation.
>
> However, the police decide that details about the person's medical absences are not relevant to the current investigation.
>
> As the primary purpose for processing details of the person's medical absences is for human resources reasons, the police deal with the SAR under the UK GDPR.

You may incidentally collect some irrelevant information, if you collect bulk information for a law enforcement purpose (eg to investigate a crime). As you can only process personal information collected for law enforcement purposes under the UK GDPR in limited circumstances, information which is irrelevant to your law enforcement purpose will not automatically fall within the UK GDPR regime. Therefore, you should continue to deal with the information under Part 3.

If someone makes a SAR "for all the information you hold about me", you **must** deal with their entire request under Part 3, not just those elements of the SAR that relate to your criminal investigation. Obviously, if you already hold some of the information about the person under the UK GDPR, then you **must** deal with this part of the request under the UK GDPR.

> **Example**
>
> Police seize a number of laptops and phones from a person for the purpose of investigating allegations that they possess images depicting child sexual abuse. Having determined that it is strictly necessary to do so, police extract the information stored on the devices. On reviewing the extracted material, they find some incriminating evidence, but also a large amount of other information, including the person's own bank and credit card details, some health information,

and family photographs. Some of this information is not relevant to the offences under investigation.

They are still processing the information they collected incidentally (such as bank details, health data and family photos) under Part 3. This is because the primary purpose for collecting the information was for a law enforcement purpose. The person makes a SAR for all the information the police have extracted from their devices. However, the police are still sifting the information, to decide if it's relevant to the investigation.

Just because some of the information is unlikely to be relevant does not bring it within the remit of the UK GDPR. The primary purpose of processing the information is for investigating crime, and the police should deal with the SAR under Part 3.

Although you may not have any use for irrelevant information, you **must** still store it in line with your retention and disposal schedule (at least until you have completed sifting it to decide if it is relevant). In general, if information is irrelevant for your law enforcement purposes, you **must** limit its further use, where possible, and ensure you don't keep it longer than necessary. You may also need to consider other regulations governing the use and retention of law enforcement data.

At what point do we decide which SARs regime applies?

You **should** usually consider the SAR under the regime you are using to process the information at the time you receive the request.

For example, if you receive a SAR for information you collected for a law enforcement purpose several years ago but you are now using it for general purposes, you should usually consider the request under the UK GDPR, and not Part 3. However, this will depend on the circumstances, and you **should** adopt a pragmatic and flexible approach.

If your primary reason for processing changes after you receive the request and before you respond, it is usually appropriate to consider the SAR under the regime that applied on the date you received the request. It may be impractical to change SARs regimes after you have received and logged the request. However, you **should** take a flexible approach and take the specific circumstances of the request into account.

You **should** always document the reasons for your decision.

Example

A financial regulator is processing an application for registration. It receives a SAR from the applicant on 9 March for "all the information you hold about me." The regulator logs the SAR. On 16 March it discovers evidence of fraudulent activity by the applicant.

The staff processing the application send the file to their enforcement department. The file then becomes part of a criminal investigation. The original purpose for processing the application was for general purposes. However, as soon as the file passes to the enforcement department to launch a criminal investigation, the primary purpose for processing becomes for one of the law enforcement purposes – the investigation of crime.

However, the regulator must still comply with the SAR they received on 9 March. It should generally consider the SAR under the UK GDPR – which was the relevant regime at the time the request was received. It may also consider whether it's appropriate to apply a UK GDPR exemption (eg crime and taxation) to the information it is now processing for a criminal investigation. The regulator should consider liaising with the enforcement department before responding to the request, if there is a risk that disclosing the information may, for example, prejudice the investigation.

Depending on the circumstances, the regulator may decide that it would be appropriate to deal with the request under Part 3 instead. If it does take this approach, it **must** be able to justify why it is taking this approach.

Do we need to provide information processed for logging purposes?

In some circumstances, yes.

Logs of information are likely to contain specific metadata about your processing activities, including exact times and dates on which certain processing actions were performed. You **must** consider, in the circumstances of the request, whether this is personal information of the person whose record the log relates to.

Logs of information create an audit trail of the information processing operations carried out by your employees. Therefore, they are likely to include the personal information of employees, including their name, and the date and time they consulted a particular piece of information.

Example

The police suspect that a member of staff has inappropriately accessed the Police National Computer to stalk and threaten another person. The staff member makes a SAR for all the information held about them. As the logs of information include their personal data, this information is potentially disclosable.

However, as logs of information may be used for the purpose of criminal proceedings, the police consider whether they need to restrict the staff member's right of access to avoid prejudicing the investigation.

If you receive a SAR for logs of information you keep further to your obligations under section 62 of the DPA 2018, you **should** use Part 3 to deal with it. For example, you may keep logs to audit and monitor your employees' activities.

Example

An employee makes a SAR, and asks for "all the information you hold about me". Most of their personal information is contained within their human resources records that you are processing under the UK GDPR. However, you also hold information about them in other databases and in your information logs.

The information logs contain the employee's name, the dates and times they accessed electronic criminal records and details of any amendments the employee made to the records.

As the information logs contain the employee's personal information, you should consider disclosing this information to comply with the SAR. However, it may be necessary to redact any information about third party individuals, (eg information about the person whose records were accessed by the employee).

Although you are not specifically processing this for a law enforcement purpose, you are doing so to comply with the logging requirement under section 62 of the DPA 2018. As such, your underlying purpose is for law enforcement. Therefore, you must deal with this element of the SAR under Part 3.

Remember that you may need to explain information to people if it is in coded form or may not be easily understood.

How do we deal with requests for unstructured manual records?

Unstructured personal data is manual information that is not, or is not intended to be, part of a "filing system".

You **should** interpret the term, "filing system" broadly. It can cover the personal information you collect for your law enforcement purposes, if it is structured according to specific criteria. This means you **should** order it in a way that allows you to easily retrieve the information. However, it does not have to include data sheets, specific lists or other search methods.

Most of the manual information you process for any of the law enforcement purposes will be structured, and therefore form part of a filing system. For example, witness statements and any other evidence used for criminal proceedings. In general, unstructured manual data is only likely to include paper records, such as loose written notes or post-it notes.

Example

Police seize large volumes of paper records to investigate money laundering. This includes notebooks, folders, and loose pages, that all contain personal information. The police store this information in boxes marked with reference numbers that relate to the investigation.

As the information is clearly referenced, it forms part of a filing system, even though some of the documents are in the form of loose notes, and the police have not yet had an opportunity to review it fully. This information is not unstructured manual data because it is clearly referenced and linked to a specific investigation.

If the police receive a SAR for this information, they should deal with it under Part 3.

You **must not** use the Part 3 SARs regime for responding to requests for unstructured manual data obtained for law enforcement purposes. Instead, you should use the UK GDPR SARs regime to deal with **all** requests for unstructured manual data, even if you have obtained the information in connection with your law enforcement purposes.

This is because Part 3 only covers personal information that:

- is processed wholly or partly by automated means; or
- is, or is intended to, form part of a filing system.

This means that unstructured manual data obtained for law enforcement purposes is not included in the Part 3 processing regime. However, it **automatically** comes within scope of the UK GDPR – provided the organisation is a public authority.

Article 2(1A) of the UK GDPR says that:

> "This Regulation [the UK GDPR] also applies to the manual unstructured processing of personal data held by an FOI public authority."

Therefore, unstructured manual data obtained for law enforcement purposes is automatically caught by this provision.

Example

Someone makes a SAR to their local authority for "all the information you hold about me".

In searching its records, the authority finds an employee's handwritten notes made to assist them in typing up a penalty notice. This was served on the person several weeks ago, and required them to pay a fine. The notes contain the person's name, and various other personal details about them that were not included in the typed up penalty notice given to the person.

As the note is unstructured, the local authority should not consider it under the Part 3 SAR regime. Instead, the authority deals with the SAR under the UK GDPR. However, the authority also takes into account the fact the note relates to an ongoing criminal matter. The authority should consider whether the crime and taxation exemption (under the UK GDPR) is relevant.

Relevant provisions in the legislation - See UK GDPR Article 6 and Recitals 40-41, 44-49, and 50

External link

See DPA 2018 sections 29(1), 36(4) and 45

External link

Further reading – ICO guidance

- UK GDPR detailed right of access guidance
  - Do we have to respond to requests made via a third party online portal?
  - What about requests for information about children or young people?
  - What is personal data?
  - Do we need to explain the information we supply?
  - Unstructured manual records
  - What other exemptions are there?

- Guide to Law Enforcement Processing:
  - Manifestly unfounded and excessive requests;
  - Law Enforcement Processing: Part 3 DPA 2018; and sharing with competent authorities under the UK GDPR and Part 2 DPA 2018
  - Logging

What should we consider when responding to a Part 3 request?

In detail

- How long do we have to comply?
- Can we extend the time for a response?
- If both the UK GDPR and Part 3 information is covered by the SAR, can we deem the request complex and extend the deadline?
- How long do we have to deal with requests for information processed for different purposes?
- Can we clarify the request in Part 3?
- Can we stop the clock and ask for clarification?
- Can we charge a fee under Part 3?

How long do we have to comply?

You **must** comply with a Part 3 SAR without undue delay and at the latest within one month of receipt of the request **or** within one month of receipt of:

- any information requested to confirm the requester's identity; or
- a fee (only in certain circumstances).

You **should** calculate the time limit from the first hour of the first day after you receive the request, fee or other requested information (whether it is a working day or not) until the last hour of the corresponding calendar date in the next month.

> **Example**
>
> If you receive a request on 30 June the time limit will start at 00:00 on 1 July and the deadline will be 23:59 on 1 August.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last hour of the last day of the following month.

> **Example**
>
> If you receive a request on 30 May the time limit will start at 00:00 on 31 May but the deadline will be 23:59 on 30 April.

If the corresponding date falls on a weekend or public holiday, you have until the last hour of the next working day to respond. This means that the exact number of days you have to comply with a request varies, depending on the month in which someone makes the request.

For practical purposes, if you require a consistent number of days (eg for operational or system purposes), you **could** adopt a 28-day period. This ensures that you always comply within a calendar month.

As the time limits are different in the UK GDPR, you **could** apply the shorter time limit (under the UK GDPR) to all SARs you receive. See How long do we have to comply? for UK GDPR details.

Can we extend the time for a response?

Unlike the UK GDPR, Part 3 does not allow you to extend the period for responding to either complex requests or a number of requests from the same person.

Section 54(2) allows for the Secretary of State to specify a longer time period for responding to SARs by way of regulations. However, at present there are no regulations in place. Therefore, you **must** respond to Part 3 SARs within one month.

If both the UK GDPR and Part 3 information is covered by the SAR, can we deem the request complex and extend the deadline?

No. You may only consider a mixed SAR to be complex for the information you process under the UK GDPR.

Therefore, you **must** provide the Part 3 information within the one month deadline, even if you have extended the time limit for responding to information processed under the UK GDPR.

However, if you wish to provide all the information at the same time, you **must** ensure that you comply with the request under the normal time limits for responding to a Part 3 SAR.

How long do we have to deal with requests for information processed for different purposes?

There may be circumstances when you need to consider requests for information processed under both the UK GDPR and Part 3. You may be using some of the information for a law enforcement purpose (eg a criminal investigation), and some of it for general purposes (eg human resources reasons).

As the time limits differ between the UK GDPR and Part 3 (and there are no provisions in Part 3 to extend the time to respond), sometimes you may need to provide separate responses.

However, you are not required to provide the information separately, as long as you clearly explain whether you are disclosing the information under the UK GDPR or Part 3 (although this may not always be possible if you need to restrict the person's right of access to this information). Where possible, you **should** provide all the information at the same time, and within the shorter time limit. This ensures that you comply with the statutory time limits for both the UK GDPR and Part 3.

Example

A local authority receives a SAR for "all the information you hold about me". It needs to provide the information it holds about the person under both the UK GDPR and Part 3 SARs regimes.

The authority has deemed the UK GDPR information to be complex, as it processes a large quantity of information about the person, and it is unclear from the request what the person is actually looking for. Therefore, it extends the time limit for responding to this element of the request by two months. However, the authority is aware it must provide the Part 3 information within one month.

The authority holds a number of documents which contain personal information that it processes about the person under both the UK GDPR and Part 3. The authority considers that it would be impractical and costly to extract the UK GDPR and Part 3 information from the documents. The authority decides it would be much more efficient to provide the person with copies of the documents.

However, although they have extended the deadline for responding to the request for the UK GDPR information, the authority must ensure it provides copies of all the personal information contained in the documents within the Part 3 timeframe.

Can we clarify the request in Part 3?

Yes. You **could** ask someone to provide additional details about the information they want to receive, such as the context in which you may have processed it, and the likely dates when processing occurred. For example, if you hold a lot of information about the person, and their request is vague, you may want to ask them to clarify what information they are requesting.

However, you cannot require someone to narrow the scope of their request, as they are entitled to ask for all the information you hold about them. If someone refuses to provide any additional information or does not respond to you, you **must** still comply with their request by making reasonable searches for the requested information. See our UK GDPR guidance on the right of access – 'What efforts should we make to find information?' for details about the extent to which you must search for information.

However, unlike under the UK GDPR, **the time limit is not paused** while you wait for a response. So you **should** ask for clarification as soon as possible.

Can we stop the clock and ask for clarification?

If you process information under both the UK GDPR and Part 3, you can only pause the time limit while you ask for clarification about the UK GDPR information.

As the clock does not stop for the Part 3 information, you **must** provide it, or if relevant, make the person aware that you have restricted access to it, within the one month time limit.

Example

An employee of the Land Registry makes a SAR "for all the information you hold about me concerning disputes or investigations".

The Land Registry processes a large volume of information about the person, as they were involved in a number of disputes and investigations, some of which are still ongoing. They were involved in a property dispute with their next-door neighbour several years ago. There was a grievance between them and other employees, and the person made a complaint to the Land Registry about its handling of a freedom of information request. They are currently buying a house and the Land Registry is investigating allegations of fraudulent activity on the part of the vendor. The fraud investigation is being dealt with under Part 3 and the file contains personal information about the person. It also contains various complaints from the person about the handling of the case.

It believes it is genuinely necessary to seek clarification as it's not clear what information the person wants, and the Land Registry processes a large volume of information. It decides to stop the clock under the UK GDPR to ask the person to specify what information they are looking for.

The clock does not stop for the Part 3 information, so the Land Registry must respond within the time limit. However, since there is a mix of information on the fraud file, including various complaints from the person, it decides that the Part 3

information is not separately searchable from the UK GDPR information. The Land Registry provides the information about the fraud matter within the usual Part 3 timescale for responding.

Can we charge a fee under Part 3?

In most cases, you **must not** charge a fee to comply with a SAR. You **must** provide the information free of charge.

However, if a request is manifestly unfounded or excessive, you **could** charge a reasonable fee for the administrative costs of complying with it, rather than refusing to comply with it. You **could** also charge a reasonable administrative fee for providing further copies of your SAR response. See our guidance on Part 3 manifestly unfounded and excessive requests.

Section 53(4) of the DPA 2018 allows for the Secretary of State to specify limits on the fees that organisations may charge to deal with a manifestly unfounded or excessive request. However, at present there are no regulations in place. It is therefore your responsibility, as a controller, to ensure that you charge a reasonable rate.

Relevant provisions in the legislation - See DPA 2018 sections 29(1), 38(3), 54(2) and 62

External link

Further reading – ICO guidance

- What is personal data?
- Guide to law enforcement:
  - Categorisation
  - Logging
- UK GDPR detailed right of access guidance:
  - How long do we have to comply?
  - Can we ask for ID?
  - Can we clarify a request?
  - What should we do if we refuse to comply with a request?
  - Can we deal with a request in our normal course of business?
  - What efforts should we make to find information?
  - Do we need to explain the information we supply?

How should we supply Part 3 information to the requester?

In detail

- What information must we supply under Part 3?
- In what format should we provide the information?
- What should we do if the information exists in different forms?
- Can we provide remote access?
- In what circumstances can we provide someone with access to their information but not a copy?
- Do we need to make reasonable adjustments for disabled people?

What information must we supply under Part 3?

You **must** make it easy for people to exercise their right of access. You **must** take reasonable steps to provide the information in a concise, accessible form, using clear and plain language.

Once you locate and retrieve the relevant personal information for the request, you **should** provide people with a copy of their information, where possible. Although you **must** respond to the request in writing, you **must** also ensure that you provide the information in a clear and accessible format. It may not be reasonable to provide the information in writing if it does not convey the true context or content of the information. For example, a transcript of a video recording. In these circumstances, you may provide the information in its existing format.

If you are unable to provide a copy of the information, you **must** still ensure that the person is able to access their data. For example, you **could** make arrangements with them to view the information you hold.

Example

A person was captured on CCTV footage and, as a result, was arrested for a public order offence. They were then interviewed under caution and released without charge. The person writes to the police to request a copy of the CCTV footage.

As the information does not exist in written form, the police provide them with a copy of the recording, having redacted the personal information of others. Alternatively, the police could have made arrangements to allow the person to

view the footage at a mutually convenient time (eg if it was not possible to provide a copy, or the person agreed to view the footage instead). Depending on the circumstances, it may be necessary to redact the personal information of other people, before providing the person with access to the footage.

People need a reasonable amount of time to review and assess the information you hold about them. So, if they attend your premises in person, you **should**, where possible, provide them with enough time to consider this information.

If you process information electronically, you **must** ensure that your software has been built with accountability and security measures in mind. As controller, you **must** comply with all of your data protection obligations. This includes the right of access, and any of the other individual's rights. For example, you may need to redact the personal information of a third party before responding to a SAR. This is particularly important if the information concerns children or vulnerable people, including witnesses or victims. Therefore, it is important that your software can perform this function.

In what format should we provide the information?

How you provide the information, and the format you use, depends on how the request was submitted (ie electronically or otherwise):

- If the person submitted the SAR electronically (eg by email or social media), you **must** provide a copy in a commonly used electronic format. You **could** choose the format, unless the requester makes a reasonable request for you to provide it in another commonly used format (electronic or otherwise). (See What is a commonly used electronic format?)
- If the person submitted the SAR by another means (eg by letter or verbally), you **must** respond using the same method, where practicable. If possible, you **should** comply with a person's reasonable request to provide the information in a commonly used format, even if they've made the request using a different method.

Example

A prisoner writes a letter to the police, asking for copies of their personal information.

The police would normally send the information by electronic means. However, since the person has made the request by letter, they must print out the requested information and either hand deliver it to the prison or ensure that it is delivered securely by post.

Many people within the criminal justice system may not be able to access information in certain formats. For example, prisoners may not be able to access electronic systems, or have only limited access to electronic systems. On the other hand, they may not have a secure method of storing paper copies of their information. Under section 52(6) of the DPA 2018 you **must**, where possible, help people exercise their right of access.

It may not always be possible to provide the information in the same format as the request or in the person's preferred format. If not, you **should** contact the person, and give reasons. For example, where you have concerns about security. If the information is sensitive, you **should** transfer it to the requester using an appropriately secure method. See our UK GDPR right of access guidance How do we provide the information securely? for further details.

Remember that the onus is on you to provide the information to the person (or their appointed representative). They should not have to take action to receive the information (eg by collecting it from your premises), unless they agree to do so. However, you are not required to create new information (eg transcripts) in order to respond to a SAR. If it's not possible to provide a copy of the data, you **must** still ensure that they are able to access their information.

You **must** take reasonable steps to provide information in an accessible and easy to understand way. You **should** document the efforts you make to ensure the information you provide is accessible, including contacting the person, where appropriate. You **must** be able to provide evidence of your efforts to the ICO, if asked to.

What should we do if the information exists in different forms?

You **must** respond to requests in writing, and provide the information in a concise, intelligible, and easily accessible format using clear and plain language. If information is clear and accessible in its written form, it will usually be appropriate to provide the information in writing. However, you are not required to create transcripts if you would not normally do so.

Depending on the circumstances, you may provide the information in its original form. For example, this may be the case if:

- the person specifically requests the information in its original form (eg CCTV footage or audio recordings); or
- providing the information in writing is unlikely to fully comply with the SAR (eg if it is unlikely to communicate the full content and meaning of the personal information).

Audio or visual recordings are likely to contain further context and meaning that cannot be communicated in a transcript. For example, a person's tone of voice may display sarcasm,

anger or fear.

In these circumstances, it is good practice to discuss with the person their preferred format, before responding to the request.

Example

A person is interviewed under caution on suspicion of having aided and abetted a murder. They are offered the assistance of a duty solicitor but refuse.

After the interview, the police arrest the person, who then makes a SAR for the audio recording of the interview. The police ask them if they would be happy to receive a copy of the transcript. The person refuses, and specifically asks for a copy of the audio recording. They explain that they were extremely anxious during the course of the interview and experienced a panic attack. They believe that their symptoms led to them wrongly implicating themselves in the crime.

The person believes that the recording will help demonstrate their state of mind and mental health during the police interview. They want this information in order to obtain legal advice.

While this information is likely to be disclosed in the course of legal proceedings, the person is also entitled to make a SAR for their personal data, which includes information about their emotions, state of mind, and mental health.

Once you have responded to a request, the person may contact you and state that they believe that the response you have provided in writing is incomplete. They may ask you to provide the information in its original format. You **should** deal with the matter as part of their original request. This means you **should** respond as soon as possible to:

- provide a copy of the information in the alternative format (eg audio recording); or
- allow the person an opportunity to access their information in the alternative format, by inviting them to your premises to listen to or view the information.

In deciding what response is appropriate, you **should** carefully consider the circumstances of the request. For example, you may consider the following factors:

- Is it reasonable to ask the person to attend your premises to view or listen to the recording rather than provide them with a copy? For example, this may depend on how far they would have to travel.
- Is there a disparity between the transcript and the alternative format? If the transcript is vague, or lacks some crucial detail, you **should** provide a copy of the recording, where possible. However, the transcript may be generally comprehensive but does not

include some contextual information (eg tone of voice or facial expressions). In this case, it may be reasonable to provide the person with an opportunity to view or listen to the recording in order to check the accuracy of the transcript.
- Would providing a copy of the recording be manifestly unfounded or excessive?

You **should not** deem a request as excessive just because you have already provided the information in writing. If the response is incomplete, it may be reasonable for the person to ask you to provide it in an alternative format, as part of their original request. See our guidance on manifestly unfounded and excessive requests.

Example

A person was interviewed under caution. The police decide not to charge them. The person later makes a SAR for a copy of the audio recording. The police respond to the request by providing a transcript of the interview.

The person asks for a copy of the recording because they think the transcript is inaccurate. As the police believe that any inconsistencies are likely to be minor, they invite the person to attend the police station so they can listen to the recording to check the accuracy of the transcript.

Can we provide remote access?

You **could** provide someone with remote access to their personal information through a secure system, **if they agree** (although you **should** consider whether you need to redact any third party data).

However, providing remote access does not necessarily mean that you have provided someone with a copy of their information. This depends on whether they are able to download a copy of the information they requested. If they are able to download it from the remote access system, then you have provided them with a copy.

In what circumstances can we provide someone with access to their information but not a copy?

In most cases, you **should** provide someone with a copy of their personal information in response to a SAR. However, in certain circumstances, you **could** provide them with access to their information rather than a copy. For example, if:

- one of the Part 3 restrictions applies to the provision of a copy of the information;
- the cost of providing a copy of the information may be deemed as manifestly excessive; or

- the person agrees.

This is not an exhaustive list, and there may be other reasons why you may be unable to provide a copy of the information. You **should** keep a record of your reasons, and be able to justify your decision, if required. If necessary, you **should** redact information about other people before giving someone access to the information.

Do we need to make reasonable adjustments for disabled people?

Yes. Some disabled people may experience communication difficulties if your processes aren't fully accessible, and therefore have difficulty making a SAR. You **must** make reasonable adjustments, if a disabled person wishes to make a request. If you are not clear about what information a person is asking for, or what reasonable adjustments they need you to make, you **should** request clarification in an accessible format and send it to the disabled person to confirm the details of the request.

What is a reasonable adjustment will depend on someone's specific needs, and you **must** be clear about exactly what reasonable adjustments are required. If you are unsure about what reasonable adjustments may be necessary, you **should** communicate with the person (eg by speaking to them) before responding to the SAR to find out how best to meet their needs. This may be by providing the response in a particular format that is accessible to the person, such as large print, audio formats, email or Braille. If someone thinks you have failed to make a reasonable adjustment, they can make a claim under the Equality Act 2010 or the Disability Discrimination Act 1995 (NI). Further information about your legal obligations and how to make effective reasonable adjustments is available from the Equality and Human Rights Commission or from the Equality Commission for Northern Ireland.

> ### Relevant provisions in the legislation - See DPA 2018 section 52
> External link

Further reading – ICO guidance

- UK GDPR right of access guidance
  - How do we provide the information securely?
  - Do we need to explain the information we supply?
  - What is a commonly used electronic format?
- UK GDPR guidance on DPIAs
- Part 3 guidance on the right to be informed

Can we restrict the right of access under Part 3?

In detail

- Can we restrict access to the information we provide under Part 3?
- What is a 'necessary and proportionate measure'?
- What rights and interests may be impacted by restricting someone's right of access?
- When can we neither confirm nor deny we hold the information?
- What does "avoid obstructing an inquiry, investigation or procedure" cover?
- What does "avoid prejudicing" cover?
- What does "protect public security" cover?
- What does "protect national security" cover?
- What does "protect the rights and freedoms of others" cover?
- Can we restrict the right of access for more than one reason?
- Can we restrict the right of access for a specified period of time?
- Do we need to record our reasons for restricting someone's right of access?
- Do we need to tell people why we have restricted their rights?
- Can we rely on the UK GDPR exemptions to withhold personal information under Part 3?
- Can we withhold information on the basis of 'legal professional privilege'?

Can we restrict access to the information we provide under Part 3?

Yes. Although you must tell people whether you are processing their information, and provide access to it, there are circumstances when you can restrict this right. These are referred to as 'restrictions' in this guidance.

You could apply a restriction in full, or in part, if it is necessary and proportionate in order to:

- avoid obstructing an official or legal inquiry, investigation or procedure;
- avoid prejudice to the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security; or
- protect the rights and freedoms of others.

You should only apply a restriction to the extent that it is necessary to achieve one or more of these purposes. You must provide the person with any information that does not come within the restriction.

If you are applying a restriction, you still need to provide them with certain supplementary information, eg by providing them with a copy of your privacy notice.

When someone is not aware that you are processing their personal information, you may be able to apply a restriction to their right to be provided with specific privacy information. See When do we need to take action to enable someone to make a SAR?.

What is a “necessary and proportionate measure”?

You must only apply a restriction if it is “necessary”. This means that you must demonstrate that you have identified a reasonable possibility of a potential risk. It must be more than speculative, but doesn’t have to be a foregone conclusion. If you can reasonably achieve your purpose by another means, you should do this instead. For example, by redacting the sensitive information.

You must also demonstrate that your decision to restrict access is “proportionate”. This means that your reasons for applying a restriction must be sufficiently important to justify any impacts that restricting access will have on someone. When considering the impact on the person, you must take into account their fundamental rights and legitimate interests; and consider the actual consequences to them if you apply the restriction. You should only infringe the person’s rights to the minimum extent necessary to achieve your purpose.

In general, you should consider all relevant factors and carefully balance the person’s right of access against your reasons for restricting access. The amount of weight you attach to the person’s right of access depends on how compelling their need to have access to the information is. If you are unsure of the motivation behind the request, you should take into account:

- the nature of the requested information;
- how you have categorised the person’s personal information; and
- why you are processing it.

You should balance the rights of the person against the harm disclosure may cause. The amount of weight you attach to any person’s rights, freedoms or legitimate interests may depend on how compelling or trivial they are, and on how compelling the need to restrict the right of access is.

You could restrict access to some or all of the information depending on the circumstances. As you must only restrict access to the extent necessary to achieve your purpose, you should generally provide as much information as you can – eg by redacting the sensitive data and providing the person with the rest of the information.

In certain circumstances, restricting access will have such an adverse impact on a person's rights, that you may not be able to justify it as "a necessary and proportionate measure". In other cases, it will be reasonable to restrict access, even if the person's rights are adversely impacted. This is the case if the underlying purpose of the restriction is compelling, and there are no other ways to mitigate the risks you have identified.

Ultimately, you should make a reasoned and sensible decision based on genuine risks. You should keep a record of your decision, and be able to justify your position and provide details to the ICO, if asked to. You should explain your reasons to the person, where possible.

Example

An employee is injured at work and the health and safety regulator launches a criminal investigation. The employee makes a SAR to the regulator asking for all the information held about them. They want to use the information to obtain legal advice about their chances of bringing a successful personal injury claim against their employer.

The regulator is concerned that disclosure of certain information may be prejudicial to the investigation. Also, if some of the information were to reach the media, this may have an impact on the fairness of any future trial. However, the person has a legitimate interest in wanting to access the information, as this may help them decide whether or not to make a claim.

The regulator must balance the person's rights against the possible prejudice to the investigation in disclosing the information. The regulator documents the impacts of disclosure against the impacts on the person of restricting access. It carefully considers any relevant factors and records how it has reached its decision.

For example, refusing to provide the information will not prevent the person from obtaining legal advice. However, the legal advice will be based on more limited information. It also considers that it will only be necessary to restrict access for a certain length of time, and once the investigation has ended, the regulator will be able to provide the information

What rights and interests may be impacted by restricting an individual's right of access?

You **should** consider the rights, freedoms and interests of people broadly. Restricting access to personal information can impact any aspect of an someone's life, and not just in the context of criminal proceedings.

For example, refusal to provide the information may impact fundamental rights and freedoms, such as:

- the right to a fair trial;
- the right to liberty and security;
- the right to respect for private and family life;
- freedom to choose an occupation and the right to engage in work; or
- freedom to conduct a business.

Which of the person's rights and interests are impacted will vary depending on the circumstances, and how you have categorised them.

When can we neither confirm nor deny we hold the information?

Even if you refuse to provide access to requested information by applying a restriction, in most instances you **must** confirm whether or not you hold the information.

However, if disclosing whether you hold the information may undermine the purpose of restricting the right of access in the first place, you can restrict the individual's right to know whether you are processing their information – by refusing to confirm or deny whether you hold their information. This is often called a "neither confirm nor deny" (NCND) response.

Again, you **must** only apply a restriction if it is necessary and proportionate to do so, taking into account the person's fundamental rights and interests.

The decision to neither confirm nor deny is separate from a decision to restrict access to the information. You **should** make this decision entirely on its own merits. There may be circumstances when an NCND response may not be a necessary or proportionate measure.

Example

The police are investigating a murder. They suspect a person is involved and place them under surveillance, without their knowledge.

This person makes a SAR for any information held about them relating to the murder investigation. The police restrict access because disclosure is likely to prejudice their investigation.

The police must separately consider whether to confirm or deny they hold the person's personal information. Since the person is not aware they are under surveillance, the police are likely to undermine the purpose of restricting access if they confirm that they hold any information. This is because the police have reasonable concerns that the person may alter their behaviours and movements if they know they are under investigation. They may also attempt to conceal evidence or take action which could prevent the apprehension of a suspect.

The police therefore respond to the request by providing an NCND response. This is because confirming the information is held would undermine the reason why they restricted access to the information.

Example

Another person makes a SAR to the police for any information held about them relating to the same murder investigation. The police do not hold any information about this person, but are aware they are acquainted with the suspect. Informing this person that they do not hold information about them may undermine the investigation. This is because there is a risk that they may discuss their response with the suspect, and enable them to draw inferences from the different responses they received. The police issue an NCND response.

What does "avoid obstructing an inquiry, investigation or procedure" cover?

You **could** restrict access to some or all of the information you hold, if disclosing it would obstruct an official or legal inquiry, investigation or procedure. This can include any public investigation or inquiry and not just criminal investigations or proceedings. However, this is only if you are processing the information for a law enforcement purpose. For example, depending on the specific context and circumstances, it **could** apply if disclosing the information would obstruct an ongoing or future coroner's inquiry.

"Obstructing" means preventing or delaying an inquiry, investigation or proceedings from taking place or progressing within a reasonable time.

You **could** restrict the person's right of access, if you believe that complying with the SAR may frustrate, or cause difficulties or impediments in progressing an inquiry, investigation, or other official or legal procedure. However, you cannot restrict the person's right of access just because a SAR is inconvenient, time-consuming, or there are ongoing proceedings. You **must** be able to demonstrate why restricting the right of access is

necessary and proportionate.

Example

A person is arrested and questioned by police in connection with a public order offence. The police believe they are a member of a violent gang under investigation for numerous offences. The police do not have enough information to detain the person in custody but investigations are ongoing. The person requests all the personal information the police hold about them.

The police are concerned about releasing some of the information to the person, in case they share it with other gang members, who are potential suspects. The information might alert them to what the police already know about their activities, which could allow them to evade capture or cause them to engage in further criminal activity.

The police want to restrict access to the information on the basis that disclosure could obstruct the ongoing investigation. They decide that the impact to the person is minimal as they have not been charged with an offence due to lack of evidence, and so failure to disclose the information does not impact their rights.

The person is therefore only entitled to the information that has not been restricted. The police document their reasons for restricting access. They advise the person that disclosing the information would harm ongoing investigations, but do not provide any specific details as this would undermine the purpose of restricting access.

What does "avoid prejudicing" cover?

You **could** restrict access to some or all of the information you hold if providing it may prejudice:

- the prevention or detection of crime;
- the investigation and prosecution of criminal offences; or
- the execution of any criminal penalty.

In the context of criminal justice, "prejudice" can have different meanings depending on the context and circumstances.

In the context of the prevention, detection, and investigation of crime, prejudice may occur where disclosing the information may undermine an inquiry. For example, by revealing details about a covert policing operation. It may also be relevant if you have reasonable grounds to believe that disclosing information to a suspect could lead to them taking steps

to conceal a crime.

Prejudice, in this context, can also mean preventing an investigation from being conducted independently or fairly. For example, if disclosing the information would impair or damage the rights of anyone under investigation or charged with an offence.

Prejudice can also apply in the context of the "execution of criminal penalties". This term is not specifically defined in the legislation but generally means any measure or process used to determine an appropriate penalty for an offender. This may include sentences handed down by a judge or out of court disposals. For example, it may be relevant if a judge is deciding whether to sentence an offender to a term in prison or community service. However, it may also apply in the context of a police caution or conditional discharge, for example.

In the context of court proceedings, including sentencing proceedings, prejudice can occur if decision-makers make a decision:

- before considering the evidence in full;
- based on unfair, irrelevant or inadmissible evidence; or
- based on irrelevant circumstances or preconceived opinions.

Example

The victim in a high profile criminal trial requests all the personal information the prosecution service hold about them. This includes witness statements and other evidence gathered by the police, including notes and the opinions of senior officers about the facts or circumstances.

Some of this evidence will not be admissible in court. The rest will need to be properly tested during the course of the trial.

If the prosecutor provides the information to the victim, they cannot control what they do with it. If it's disclosed to the media, it could prevent the defendant from having a fair trial.

As the victim will be compelled to testify at court, there is also a risk that providing them with this information may affect their testimony. This is because they may use it to help them reconstruct their version of events rather than basing their testimony on their own recollection.

The prosecution service considers the rights of the victim in deciding whether to provide them with access to this information. However, they decide that restricting access to some of the information is a necessary and proportionate measure to ensure that the defendant is tried fairly. They decide that the balance

weighs against disclosure in these circumstances.

What does “protect public security” cover?

You **could** restrict a person’s right of access to their information if you consider it to be a necessary and proportionate measure to protect public security.

“Public security” generally concerns the welfare and protection of the public at large. It may cover the protection of life, institutions and organisations against public threats, crime, disasters and other threats to life, safety and well-being. For example, it may include:

- use of intelligence to address possible threats;
- policing large events; and
- investigating drugs offences, human trafficking, or institutional child abuse.

Public security can encompass most major public policy issues, or anything that threatens public order.

Example

The police are investigating the activities of a criminal gang operating in the local area. This includes violent crime, drugs, and human trafficking offences. They arrest someone on suspicion of affray. The police have CCTV footage of the incident. The person wants to view this footage, and makes a request for “all the data you hold about me”.

The police also hold information that suggests the person is connected to the criminal gang they are investigating. However, they currently do not have sufficient evidence to establish the person’s involvement. They are concerned that if they disclose this information there is a risk that the person might alert other members of the criminal gang who are still at large. They are also concerned that disclosure could risk the life and safety of victims.

Taking this into account, and having considered the impact on the person’s rights, they decide to restrict access to the information that links the person to the activities of the criminal gang. This is based on the need to protect public security.

However, as the incident of affray does not relate to these activities, the police do not need to restrict the person’s access to the CCTV footage. They disclose this information after redacting any personal information about third parties.

What does “protect national security” cover?

You **could** limit or restrict the right of access where this is a necessary and proportionate measure to protect national security.

“National security” is generally understood to cover the security and well-being of the UK as a whole, its population, and its institutions and system of government.

See our guidance on the national security provisions.

What does “protect the rights and freedoms of others” cover?

You **could** restrict a person’s right to access their personal information if you consider it is a necessary and proportionate measure to protect the rights and freedoms of others. This is usually relevant if the information contains personal information about someone else.

See, What should we do if the Part 3 request involves information about other people?’.

Can we restrict someone’s right of access for more than one reason?

Yes. However, if you need to restrict access for more than one reason, you **should** be able to explain why this is necessary and proportionate, and keep a record of your reasons.

Example

The police are investigating a crime. The person under suspicion makes a SAR for their personal information. The police believe that disclosing it is likely to:

- prejudice the investigation;
- present a risk to public security; and
- place another person at risk.

The police decide to restrict the person’s right of access on the basis of sections 45(4)(b), (c), and (e).

However, they **should** consider each of their aims separately, and be able to explain in sufficient detail, why applying a restriction to the person’s right of access to their information is necessary and proportionate in the circumstances.

Can we restrict the right of access for a specified period of time?

Depending on the circumstances, you **could** apply a restriction to the person’s right to access their information for a specific length of time. For example, until an investigation is

complete or criminal proceedings have ended.

You are not required to keep a SAR open after you have applied a restriction and responded to the person. However, if you only need to restrict someone's right of access for a specific length of time, you **could** inform them when they may be able to resubmit their request, if possible.

Do we need to record our reasons for restricting someone's right of access?

Yes. You **must** record your reasons for restricting, either wholly or partly, someone's right of access to the following information:

- confirmation of the processing (ie if you have issued an NCND response);
- any of their personal information;
- any of their supplementary information; and
- certain privacy information.

You **should** also record why you have decided this measure is a reasonable and proportionate response to an identified risk. You **must** be able to make this record available to the ICO, on request (although you should only keep personal information in accordance with the terms of your retention and disposal schedule).

You may find it helpful to refer to our Accountability Framework – see the section on Logging and tracking requests.

Do we need to tell people why we have restricted their rights?

In most cases, if you have restricted someone's right to access their information, you **must** inform them as soon as possible about:

- the reasons why;
- their right to make a complaint to the ICO; and
- their ability to seek to enforce this right through the courts.

You do not need to explain that you have restricted their right of access or why, if this undermines the purposes of restricting the right in the first place. However, where possible you **should** be transparent about your reasons for restricting their right of access to their personal information.

Can we rely on the UK GDPR exemptions to withhold personal information under Part 3?

No. If you are processing information for law enforcement purposes, you cannot apply the UK GDPR exemptions.

Other rules apply to legal professional privilege – see the next section, Can we withhold information on the basis of legal professional privilege?.

Can we withhold information on the basis of legal professional privilege?

There is no specific restriction under Part 3 of the DPA 2018 that says you may withhold information on the basis it is protected by legal professional privilege.

However, legal professional privilege is an established common law principle. Clients have a fundamental right to seek and obtain confidential legal advice, without the risk of such details being disclosed to others. Therefore, you may withhold information on the basis of the common law principle of legal professional privilege.

Example

The prosecution service decides that it has sufficient evidence to prosecute someone for several offences. However, due to numerous complexities in the case, the prosecution service decides to obtain legal advice before proceeding.

The person makes a SAR for any information the prosecution service holds about them, including any advice or reports obtained. The prosecution service decides that the legal advice is protected by legal professional privilege. This is because it is a confidential communication between client and lawyer, made for the purposes of obtaining legal advice.

The prosecution service does not need to consider whether any of the information contained in the legal advice is disclosable as privilege applies to all the legal advice. The prosecution service withholds the legal advice completely.

Relevant provisions in the legislation - See DPA 2018 section 45

External link

What should we consider when acting as joint controllers?

In detail

- What do we need to consider if we are acting as joint controllers?
- What are the responsibilities of the "contact point"?
- Do we need to consult with joint controllers before responding to a SAR?
- What happens if we are only processing some of the requested information for joint purposes?
- Can we consult other competent authorities when deciding whether to apply a restriction?
- What happens if independent controllers are processing the same information for different purposes?

What do we need to consider if we are acting as joint controllers?

Where two or more competent authorities jointly determine the purposes and means of processing personal information, they are acting as joint controllers.

If you are acting as a joint controller, you **must**:

- have an arrangement in place with your fellow joint controllers that clearly and transparently sets out each of your responsibilities under Part 3, including how you deal with SARs; **and**
- specify a contact point that is one of the joint controllers.

Example

Separate policing organisations have statutory remit to enter into a collaboration agreement to investigate serious crime. The agreement sets out the respective functions of officers and staff at each organisation.

As the organisations are processing personal information as joint controllers, they must have joint arrangements in place that allocate each organisation's data protection responsibilities.

What are the responsibilities of the "contact point"?

Joint controllers **must**, in their joint arrangements, name one of the joint controllers as the contact point. You **must not** appoint a third party as the contact point or have more than

one contact point.

Each joint controller **should** name the contact point on their websites or in other communications, and direct people to make their SAR to the named contact point, where possible. However, a SAR is received as soon as it is received by any of the joint controllers.

If any of the joint controllers receives a SAR, you **should** forward it to the contact point as soon as possible. Your joint arrangements **should** make provision for this. In general, you **should** make each joint controller aware of every SAR.

The joint arrangements **must** clearly set out the duties of each joint controller about SARs. The contact point often takes responsibility for all aspects of complying with the SAR (including performing reasonable searches, redacting, and providing (or refusing) the information). However, these duties may be allocated amongst the joint controllers. The contact point **could** coordinate responses to a SAR, by liaising with the other joint controllers, as appropriate, subject to the terms of the joint arrangements.

Your joint arrangements **should** make it clear if people can make a SAR to each controller, or to the contact point only. Your arrangements **should** also set out who people may complain to, if they are unhappy with your response. Each controller **must** comply with their specific responsibilities under the terms of the joint arrangements and also with their statutory data protection obligations.

While you **must not** delegate the role of the contact point to a third party organisation, this does not prevent joint controllers from outsourcing certain aspects of your SAR work to a processor (eg performing reasonable searches).

Do we need to consult with joint controllers before responding to a SAR?

Depending on the circumstances, you **could** seek the views of other joint controllers about how you respond to a SAR. You **should** include provisions in your joint arrangements for notifying other joint controllers before responding to a SAR.

Example

Two government agencies (Agency A and Agency B) use shared information access systems to process personal information for law enforcement purposes. They are acting as joint controllers. Their arrangement specifies that Agency A is the contact point for SARs and is responsible for responding to them. The arrangement also states that Agency A will consult with Agency B to decide how to respond to a SAR.

Agency A receives a SAR.

Agency A informs Agency B about the SAR and seeks its views before deciding how to respond. Agency B believes disclosing some of the information may put another person at risk. It believes that it is necessary and proportionate to apply a restriction (to protect another person), and provides evidence to support this.

As set out in the joint arrangement, Agency A is responsible for complying with the SAR. It should carefully consider Agency B's arguments, to decide whether it should apply the restriction (including whether it is necessary and proportionate to do so).

On the basis of the joint arrangement, Agency A may be subject to enforcement measures by the ICO if it does not agree with the use of the restriction. However, Agency B may be required to assist with the ICO's investigations.

What happens if we are only processing some of the requested information for joint purposes?

There may be circumstances where a number of organisations are acting jointly about one aspect of their processing. However, they may be acting independently in carrying out other processing activities.

If some of the information falls within scope of the joint arrangements, the joint controllers with responsibility for responding to SARs **must** deal with this part of the SAR.

Example

A number of organisations (Agency A, Agency B, Agency C, and Agency D) are able to access a shared database that contains information about people's criminal convictions. Agency C owns and manages the system on behalf of the other agencies. The information is processed under Part 3.

Each of the agencies is an independent controller in its own right. However, they are joint controllers for the information stored on the shared database. Agencies A, B, C, and D have joint arrangements that set out each of their data protection responsibilities under the DPA 2018, including their arrangements for dealing with SARs.

The arrangements specify that Agency C is the contact point and responsible for responding to SARs.

Agency D receives a SAR from someone requesting "all the information you hold about me". Agency D is an independent controller for most of the information it processes about the person. However, the information held on the shared database is also within scope of the request. As Agency D is not the contact point for the information held on the shared database, it forwards the SAR to the named contact point, Agency C.

Agency C must respond to the element of the SAR that concerns the information held within the shared database.

Can we consult other competent authorities when deciding whether to apply a restriction?

It depends. During the lifecycle of a criminal case, a person's personal information is likely to processed by a number of competent authorities. For example, police obtain information for the purpose of investigating crime. If the prosecution service reviews the information to decide whether or not to pursue a prosecution, but does not issue instructions about the investigation, the police and the prosecution service are working collaboratively, yet independently of each other, and make decisions separately. They are not necessarily joint controllers, but are likely to share personal information in the course of a criminal case.

There is nothing in the DPA 2018 that requires you to only consider your own specific circumstances in deciding whether to restrict access. It is not usually necessary or appropriate to consult other organisations before you respond to a SAR. However, if you believe there may be a risk of serious harm in disclosing the information, you may wish to

do so.

In these circumstances, you **should** base your decision on evidence provided by the other controller. You are responsible for complying with the SAR and **must not** restrict the right of access or speculate about risks without proper justification. You **should** be able to justify why you consider applying a restriction is necessary and proportionate. You **must** also respond to the request within one month.

If independent controllers share information with each other, you **should** have a data sharing arrangement in place.

What happens if independent controllers are processing the same information for different purposes?

There are likely to be circumstances when you and another organisation are processing the same personal information for different purposes (eg law enforcement and general purposes).

For example, a hospital shares information with police about the nature of the injuries sustained by a victim. The hospital is processing the information under the UK GDPR, while the police are processing it under Part 3.

If you are processing personal information under Part 3, you **could** apply a restriction under Part 3 of the DPA 2018. You **could** also consult other organisations before you respond to a SAR, if you have identified a potential risk of serious harm. If you consult another organisation, you **must** still respond to the request within one month of receiving the SAR.

> Relevant provisions in the legislation - See DPA 2018 section 58
> External link

Further reading – ICO guidance

- Law enforcement processing: Part 3 DPA 2018; and sharing with competent authorities under the UK GDPR – We are a competent authority. How do we share data under Part 3 of the DPA 2018?'
- UK GDPR guidance on controllers and processors and contracts

What should we do if the Part 3 request involves information about other people?

In detail

- What is the basic rule?
- What approach should we take?
- What about confidentiality?
- Does categorising people impact what information we can provide them with?
- How should we deal with requests from people who fall within multiple categories?

What is the basic rule?

Personal information can relate to more than one person. Therefore, responding to a SAR may involve providing information that relates to both the requester and another person ("third party information").

> **Example**
>
> A prisoner makes a request for all their personal information. They have recently assaulted another inmate. The prison authority's records contain personal information about the victim, witnesses, and a number of other people, including family members of the prisoner.
>
> The prison authority needs to consider the rights of the third parties when responding to the prisoner's SAR.

In such circumstances, you **could** apply the restriction set out in section 45(4)(e) of the DPA 2018. This allows you to restrict access where it is necessary and proportionate to protect the rights and freedoms of others.

In order to consider whether to apply the restriction, you **should** follow the three-step process set out below.

What approach should we take?

Step one – Does the request require disclosing information that identifies someone else?

You **should** consider whether it is possible to respond to the request without revealing information about a third party. You **should** take into account the requested information

and any information you reasonably believe the person making the request may have, or may get hold of that would identify the third party.

Depending on the circumstances, you may be able to redact the third party information, so that the other people are no longer identifiable. However, people may be identifiable from the context or circumstances, even if you redact their name or other personal details. For example, if you disclose a witness statement to a suspect, the suspect might be able to identify the witness from the general content and context of the statement.

Example

A person is arrested for assault. A witness who lives nearby has made a statement describing the attack. The person who was arrested makes a SAR for their personal information. If the witness statement is released, it is reasonably likely that the person will be able to identify the witness from the date, time, description of the incident, context and circumstances.

You **should** consider the risk to other people broadly. If you redact personal details, you **should** carefully consider whether the third party may be identifiable by jigsaw identification.

Example

A person is charged with possession of cannabis with intent to supply, after a fifteen-year-old child who lives in the area noticed the person behaving suspiciously one evening while out walking their dog. They reported the incident to police and later provided a statement.

The person makes a SAR to the police for their personal information. If the police redact the child's name and personal details, they are not obviously identifiable from the statement, or the transcript of the telephone recording when they reported the incident. However, if the police disclose any of this information, the person may be able to identify the child through jigsaw identification. For example, the child walks their dog in a specific location at the same time each day. There is also a risk that the suspect's acquaintances may have noticed the child in the area that evening.

In deciding whether to apply the restriction, the police should take into account any relevant factors. This includes the fact that the statement is likely to be disclosed in the course of criminal proceedings anyway, but under the jurisdiction of the court. The police then need to balance the rights of the person making the

SAR with the rights of the child who provided the statement.

Step two – Do we need to apply the restriction?

It may be impossible to simply remove the third party information and still comply with the request. In these circumstances, you **should** consider whether it is reasonable to apply the restriction for third party information.

Step three – Is the balance for or against disclosure?

You **must** carefully consider the rights, freedoms and legitimate interests of both the requester and the third party, when you decide whether the restriction is necessary and proportionate. You **should** consider all relevant circumstances, and in particular:

- the type of information that you would disclose;
- how you have categorised both the person making the request and the third party;
- the impact of restricting access on the fundamental rights, freedoms and legitimate interests of the person who made the SAR;
- the impact of disclosure on the fundamental rights and freedoms of the third party;
- any duty of confidentiality owed to the third party; and
- whether it may be appropriate, in the circumstances, to obtain consent from the third party.

This is an non-exhaustive list, and ultimately you **should** make this decision taking these factors into account, along with the context of the information.

Due to the sensitivities of law enforcement processing, it may not always be appropriate to ask a third party whether or not they consent to the disclosure of their information to the requester. You **should** take into account the specific circumstances of the request when making your decision.

Example

The police receive a number of reports about various incidents of domestic violence occurring within a household. These reports have been made by the complainant. The suspect has a number of previous convictions, and the police hold a large amount of personal information about them.

The suspect makes a SAR for all the personal information the police hold about them. The police apply a restriction to some of the information as disclosure may prejudice an ongoing investigation.

The police have completed their investigations into the domestic violence allegations made by the complainant. The prosecution service has decided there

is insufficient evidence to pursue a prosecution at this stage. However, the police are keeping the information on record in case the complainant makes further allegations or the situation escalates. The police understand that the suspect may not be aware of the allegations their partner has made about them.

The police balance the suspect's right to access the reports of domestic violence made about them, against the need to protect the complainant. They have concerns that disclosing the information may risk the life and safety of the complainant. Therefore, they restrict access to this information.

However, they are able to disclose some of the information they hold about the suspect. This information does not relate to the domestic violence allegations and therefore does not present a risk to the complainant or prejudice the ongoing investigations.

What about confidentiality?

Confidentiality is one of the factors you **must** take into account when deciding whether to disclose information about a third party without their consent. A duty of confidence arises when someone discloses genuinely confidential information to you (ie information that is not generally available to the public), with the expectation that it remains confidential. This expectation might result from any statutory or common law obligations to keep certain information confidential. For example, statutory prohibitions, court orders (eg witness protection measures) or anonymity orders.

In most cases where a duty of confidence does exist, you **should** usually withhold information about a third party, unless you have the person's consent to disclose their personal information.

Does categorising people impact what information we can provide them with?

Under Part 3, organisations are required to make a distinction between personal information you use about different categories of people. This includes:

- those suspected of having committed, or being about to commit, an offence;
- those convicted of a criminal offence;
- victims and complainants; and
- witnesses or those with information about offences.

You may also hold information about contacts or associates of suspects and convicted offenders.

How you have categorised someone **could** be useful for you in deciding how to respond to a SAR. In particular, it may be relevant when you are thinking about whether to apply a restriction, in considering risk and proportionality, and balancing people's rights.

Example

The key witness and victim in a criminal investigation both make a SAR to the police for their personal information. Some of the information held is about both people. The police need to separately consider whether they can disclose this information to each person.

In responding to the SAR made by the key witness, the police consider whether to withhold the information. While there are a number of reasons why they think the key witness has a right to the information, the police ultimately decide against disclosing it.

In responding to the SAR made by the victim, the police consider whether to withhold the information. In this instance, they decide that any impact to the key witness is minimal and disclose the information to the victim.

In different circumstances, the police might decide that they should disclose the information to the key witness but not the victim. For example, if the key witness needs the information to obtain legal advice.

However, you **should** consider the particular circumstances of the request, regardless of how you have categorised people.

Example

The police hold information on their records about two next-door neighbours, Person A and Person B. There is an ongoing dispute between them about works Person A is carrying out to their property. The matter escalated one afternoon when Person B broke all the windows to Person's A's new house extension with a crowbar. Person A retaliated by physically assaulting Person B, which resulted in them needing hospital treatment. Both people were arrested.

Each person makes a SAR to the police. Some of the information being processed is about both people. In responding to each SAR, it's important that the police consider the requests separately, and weigh up the rights of each person, when they decide whether to comply.

In particular, given the nature of the incident, the police should consider whether there is a risk to either person, if they disclose their information to the other.

The police might decide to disclose the information to both people. Alternatively, they may decide that the balance weighs in favour of disclosing the information to one person, but not the other. They may instead decide not to disclose the information at all. However, the police should record the reasons for their decision.

How should we deal with requests from people who fall within multiple categories?

There may be instances when someone falls under more than one of the categories described in the above section. You may process a person's personal information in different contexts, or hold it within different files across your systems.

Example

The police process a person's personal information to investigate crime. The person is a suspect in a burglary, but is also a prosecution witness in a murder case. They are the complainant in an assault case, and the key witness in a dangerous driving case.

If someone falls into more than one category, you **must** be able to clearly identify and distinguish between these different categories for each piece of information you hold about them. If they make a SAR, you **must** identify what information their request relates to, and whether any of the restrictions are relevant to that specific information.

You can consider risk broadly. In many circumstances, disclosing personal information that relates to one case, may risk prejudicing another case. For example, it may be reasonable to restrict a person's right of access if disclosure would prejudice a separate or linked investigation. However, you **must** be able to justify why you have restricted someone's right of access in these circumstances, and you **should** ensure that any restriction is necessary and proportionate.

If you receive a SAR from someone who falls within multiple categories, you **could** ask them to explain what information they are looking for.

Relevant provisions in the legislation - See DPA 2018 sections 38(3) 44(4)(e), and 45(4)(e)
External link

Further reading – ICO guidance

For further details on dealing with requests containing information relating to a third party, see our right of access guidance – What should we do if the request involves information about other people?

Also, see UK GDPR right of access guidance – Are there any other relevant factors? to help you decide when it may be appropriate to disclose the third party information.

You may find it helpful to read our guidance on Access to information held in complaint files. While it is FOI and EIR guidance, it also covers how to deal with SARs involving third party information.

- What is personal data?
- Guide to law enforcement - categorisation of individuals

What do we need to consider if personal information is processed by a court for law enforcement purposes?

In detail

- Does someone have a right to access personal information created by a court?
- What does "by or on behalf of a court or other judicial authority" mean?
- What is a "judicial decision"?
- What information will be created by or behalf of a court for a criminal investigation?
- What information will be created by or on behalf of a court for criminal proceedings?
- What does "relating to" mean?
- What does "for the purpose of executing a criminal penalty" mean?
- Does the exception cover documents filed or placed in the custody of the court?
- Does the exception apply if the court has shared the information with another organisation?
- Is this exception time-bound?

Does someone have a right to access personal information created by a court?

A person does not have a right to access their personal information by making a SAR if it is contained in:

- a judicial decision; or
- in another document created by or on behalf of a court or other judicial authority in connection with:
    - a criminal investigation; or
    - criminal proceedings, including proceedings for the sentencing of an offender.

The DPA 2018 describes this information as "relevant personal data", and it is an exception from the right of access requirements. This means that you **could** automatically refuse to provide information that meets this definition.

The ICO does not regulate the processing of personal information by a person, court or tribunal acting in a judicial capacity. Such processing is overseen by other bodies with regulatory remit over those acting in a judicial capacity.

What does "by or on behalf of a court or other judicial authority" mean?

The terms “judge”, “judicial authority”, and “court” are often used interchangeably. As this exception only applies in the context of criminal proceedings, you should narrowly interpret the term “by or on behalf of a court or other judicial authority”.

The term “court or other judicial authority” includes any person or organisation acting in a judicial capacity. In general, this exception to the right of access only applies if the controller is a judge, magistrate, or other judicial authority **and** they are processing the information for a criminal case, including sentencing proceedings. As a general rule, this exception applies to judges or judicial authorities presiding over criminal cases or appeals, either alone or as part of a panel. However, it may also apply to independent judicial commissioners, if they are performing a judicial function in respect of a criminal matter. It may also include sheriffs and summary sheriffs presiding over criminal cases in Scotland.

In England, Wales, and Northern Ireland, this includes judges or judicial authorities presiding over:

- Magistrates’ Courts;
- Crown Courts;
- the Court of Appeal;
- the County Court (in Northern Ireland only);
- the High Court; and
- the UK Supreme Court.

In Scotland, this includes:

- the High Court of Justiciary;
- Sheriff Courts hearing a criminal matter;
- Justice of the Peace Courts; and
- Sheriff Appeal Courts.

It does not apply to organisations with powers to issue out of court disposals. For example, police or local authorities issuing fines, cautions or conditional discharges.

This exception does not just apply to documents created by a judge, for example notes made by the judge in the course of a criminal trial. It can also cover any documents commissioned by the judge or within the exclusive jurisdiction of the court. This includes documents created by non-judicial organisations **on behalf of** the court.

Example

The judge asks the Probation Service to prepare a pre-sentence report on its behalf. The judge will then use the report to determine an appropriate sentence for the convicted offender.

In these circumstances, the Probation Service is acting on behalf of the judge. The report has been commissioned by the judge, and has therefore been prepared "by or on behalf of the court".

The provision limits the circumstances when you can use the exception. It generally only applies to judicial functions (ie matters within the exclusive jurisdiction), and under the express instruction of the court.

The term "on behalf of" does not mean the same as processor in this context. If a non-judicial organisation (eg the Probation Service) acts on behalf of the court or other judicial authority, it is carrying out a delegated activity to enable the judge to carry out their judicial function (eg where it prepares a report on behalf of the judge). However, the non-judicial organisation is likely to be acting as a controller in its own right, in relation to the information it processes about the person. If it has prepared a document on behalf of the court, that document belongs to the court, and only the court may authorise its disclosure.

While the court service often acts as a processor for the judge, this exception does not apply to the administrative functions of the court, or to documents created by court staff. This is because they are not judicial functions.

What is a "judicial decision"?

In this context the term "judicial decision" means the judgment of a court in written form. However, it is not restricted to the judgment itself. It may cover any ruling or decision made by the court in the course of, or at the end of, proceedings, including:

- decisions about sentencing; or
- applications made by either prosecution or defence.

It may also include any notes, or early drafts prepared by the judge or magistrate for any of these purposes. If someone cannot make a SAR for their personal information contained in the judicial decision, where relevant, the judgment itself may be published at the conclusion of proceedings (eg following an appeal).

What information is created by or on behalf of a court for a criminal investigation?

The criminal court or other judicial authority is generally an independent decision-maker. Therefore, it does not conduct criminal investigations.

However in some circumstances, other organisations require specific approval from the court to conduct certain types of investigations. For example, judicial approval is often needed if police, or a local authority, want to conduct intrusive covert surveillance to investigate a crime.

The following are deemed to be relevant personal information:

- any decision made by the court in such cases; or
- any documents created by the judge in the course of hearing such matters (eg an application for a search warrant).

Therefore, the information does not need to be disclosed as a result of a SAR. However, this information can only be an exception from the right of access for a certain period of time. For example, until the warrant has been executed.

Example

The police are investigating a drug cartel, and suspect the involvement of a number of people. However, they do not have enough evidence to arrest anyone.

In order to investigate the crime, they want to deploy a specially trained officer to plant eavesdropping devices at the residential homes and private vehicles of the identified suspects.

However, the police require judicial approval under the relevant laws to carry out these operations. They make an application to the appropriate court. Any documents containing personal information that the judge creates in the course of hearing these proceedings is relevant personal information and does not have to be disclosed if it is subject to a SAR. However, any personal information created by the police, and lodged with the court, or used by the judge in reaching a decision, is not covered by the exception.

The DPA 2018 does not specify that this exception to the right of access only applies in the context of certain legislation. However, it is likely to be relevant if you make applications to a court to obtain judicial approval for carrying out surveillance or monitoring. For example under:

- the Regulation of Investigatory Powers Act 2000 (RIPA);
- the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A 2000);
- the Protection of Freedoms Act 2012; or
- for search warrants under the Police and Criminal Evidence Act 1984, the Police and Criminal Evidence (NI) Order 1989, or the Police, Public Order and Criminal Justice (Scotland) Act 2006.

What information is created by or on behalf of a court for criminal proceedings?

Any documents created by or on behalf of the court or other judicial authority may be exceptions from the right of access requirements. This includes those created either before, during or after the criminal proceedings. However, some information may only be excepted for a certain period of time. There may also be alternative routes for obtaining access to the information.

Therefore, you are not required to disclose records made by the court or on its behalf in the course of criminal proceedings, in order to comply with a SAR. This may include judges' notes or documents prepared in the course of a trial. For example, if the defence makes an application for some evidence to be declared inadmissible, on the basis it is not relevant to the criminal case.

Example

Counsel for the defence is acting for a person charged with possession of cannabis with intent to supply. The prosecution wants to submit evidence that the defendant has previous convictions for burglary and common assault.

The defence counsel makes an application to the court to have this evidence excluded on the basis it is irrelevant and prejudicial to the person's defence.

Any notes or other documents created by or on behalf of the court while hearing the applications made by both prosecution and defence, or in reaching its final decision, are not disclosable further to a SAR.

The exception can also cover documents commissioned by the judicial authority and created by a non-judicial organisation on behalf of the judge. This includes circumstances where a court is required by law to obtain a specific document, or the judge has exercised their discretion and orders that such a document is prepared. For example, a pre-sentence report prepared by a probation officer.

Example

In making a decision about sentencing someone who was found guilty by a jury of dangerous driving, the court commissions the probation officer to prepare a pre-sentence report on its behalf. The pre-sentence report will assist the court in determining the most suitable sentence for the defendant.

In advance of the sentencing proceedings, the person makes a SAR to the court office for their pre-sentence report. However, the court office refuses to provide the information under a SAR as it is excepted from the right of access requirements. However, it is able to provide them with a copy under other

legislation.

Access to court documents is generally covered by different rules. So even if information may not be disclosed under a SAR, there will usually be another way for someone to access the information.

For example, the defendant may be able to access their personal information under legislation that governs the disclosure of information in criminal proceedings. In England, Wales, and Northern Ireland, this is the Criminal Procedure and Investigations Act 1996. In Scotland, this is the Criminal Justice and Licensing (Scotland) Act 2010.

The personal information used to inform the document is potentially disclosable under a SAR, even if the report is not.

Example

A person is aware that a probation officer is preparing a pre-sentence report about them, in advance of sentencing proceedings. They make a SAR to the Probation Service, asking it to provide them with access to their personal information.

The Probation Service is processing information about the person that it will use to prepare the pre-sentence report. As the judge has commissioned the report, this means the report itself contains relevant personal information and is therefore excepted from the right of access requirements. However, the information used by the Probation Service to inform the report is potentially disclosable under the SAR, even though the report itself is not. Although the report may not be provided in response to the SAR, the person is entitled to see a copy of the report in the course of the proceedings.

What does “relating to” mean?

You **should** interpret the term “relating to” broadly. It is generally used to refer to information about, or linked to the proceedings. It does not just include admissible evidence, or information relevant to the outcome of the case. It can apply to most information created by, or on behalf of, a court in the course of the proceedings. This includes information that is not really relevant.

Example

During a Crown Court criminal trial, the judge makes a note of the names of prosecution and defence counsel, instructing solicitors, defendant, witnesses, the complainant, and other people present.

The judge also notes that the defence counsel is not wearing appropriate court dress for Crown Court proceedings and reprimands them, before making an adjournment.

The defence counsel makes a SAR for a copy of the judge's notes. However, the notes were made during the course of criminal proceedings. Therefore, the court can rely on the exception and refuse to disclose the note.

What does "for the purpose of executing a criminal penalty" mean?

The term "for the purpose of executing a criminal penalty" is not specifically defined, but you **should** interpret it in the general context and meaning of sections 43(3) and (4) of the DPA 2018. Since the exception typically only applies to judges or magistrates who process information in the course of a criminal trial, it generally means any sentence handed down by the court. For example, documents created by or on behalf of a court in issuing a discharge, fine, community sentence, or custodial sentence. It may also apply to courts with powers to hear appeals, for example about the length of a sentence.

It does not apply to other organisations with powers to issue out of court disposals, such as fines or cautions. Any documents created by these authorities for these purposes are potentially disclosable under a SAR.

Does the exception cover documents filed or placed in the custody of the court?

No. This exception does not cover documents filed or placed in the custody of the court.

In a criminal trial, the prosecution and defence produce and test evidence, by examining and cross-examining witnesses in order to make their case to the court. Any documents or other evidence they submit to the court is for the purpose of advancing their case. For example, witness statements, medical or forensic reports, or skeleton arguments. Although the legal representatives are duty bound not to mislead the court, they are not carrying out any judicial functions.

However, any notes or documents created by the judge during the course of the criminal proceedings will be excepted from the right of access provisions.

Does the exception apply if the court has shared the information with another organisation?

It depends. This exception does not usually apply to information the court or other judicial authority has shared with another organisation, or the parties to the case. The person may make a SAR to the organisations that received copies of the information, unless the judge disclosed it in confidence or caveated the disclosure with certain conditions. If so, you **must** take account of any court order or specific judicial instructions about the information.

Is this exception time-bound?

There is nothing in the legislation to suggest that the exception only applies until the criminal proceedings have concluded. It depends on the circumstances and the nature of the information.

For example, information may be excepted from the right of access in the following circumstances:

- until it has been disclosed under statutory or common law procedures;
- during the course of proceedings; or
- at the conclusion of proceedings (eg the pre-sentence report, and the judicial decision).

However, it is likely that certain information will be excepted from the right of access indefinitely, for example judges' notes.

> Relevant provisions in the legislation - See DPA 2018 sections 21(2), 29, 43(3) and (4), and 117
> External link

Further reading – ICO guidance

- UK GDPR right of access - unstructured manual records
- Law Enforcement Guidance – categorisation
- Guide to the UK GDPR – storage limitation

Can the right of access be enforced under Part 3?

In detail

- What enforcement powers does the ICO have?
- Can a court order be used to enforce a SAR?
- Can people be awarded compensation?
- Is it a criminal offence to destroy and conceal information?

What enforcement powers does the ICO have?

Anyone has the right to make a complaint to the ICO about an infringement of the data protection legislation in relation to their personal information. For example, if an organisation fails to comply with a SAR or their duty to give someone enough information to allow them to make a SAR.

In these circumstances, the person can ask the ICO to check that the organisation acted lawfully in refusing their SAR or restricting any of their rights.

In appropriate cases, we may take action against a controller or processor if they fail to comply with data protection legislation. For example, we could issue a controller or processor with a:

- warning;
- reprimand;
- enforcement notice; or
- penalty notice.

The ICO will exercise these enforcement powers in accordance with our Regulatory Action Policy.

Although a processor does not have any obligations under section 45 of the DPA 2018, under section 59 the controller and processor **must** have a contract in place. The contract **must** state that the processor will assist the controller with their obligations to comply with a SAR by taking appropriate technical and organisational measures, as far as this is possible (taking into account the nature of the processing).

If you are a joint controller, you are only liable to the extent you are responsible for the specific action in question, under the terms of the joint arrangements. Joint controllers **must** ensure you make appropriate joint arrangements for dealing with SARs.

Bear in mind that we may issue an information notice or assessment notice against any person.

Can a court order be used to enforce a SAR?

If you fail to comply with a SAR, the requester may apply for a court order requiring you to comply. It is a matter for the court to decide, in each particular case, whether to make such an order.

If you are a joint controller, bear in mind that a court may only make an order against you, to the extent you are responsible for the specific action in question, in accordance with the terms of the joint arrangements.

Can people be awarded compensation?

If someone suffers damage or distress (including financial loss) because an organisation has infringed their data protection rights (including failing to comply with a SAR) they are entitled to claim compensation from them. They are only able to claim compensation from the processor if it has not complied with any of its statutory obligations, or has acted outside or contrary to the controller's instructions.

If you are a joint controller, and your responsibilities for SARs are covered in your joint arrangements, you will only be liable if you are responsible for complying with the provision which has been contravened, in accordance with the terms of the joint arrangements.

Only the courts can enforce a person's right to compensation. However, they may seek to settle their claim with you directly first before starting court proceedings. You will not be liable to pay compensation if you can prove that you are not responsible in any way for the event giving rise to the damage.

Is it a criminal offence to destroy and conceal information?

Yes. It is a criminal offence to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information a person making a SAR would have been entitled to receive.

It is a defence, if you can prove that:

- the alteration, defacing, blocking, erasure, destruction or concealment of the information would have happened regardless of whether someone made a SAR; or
- you acted in the reasonable belief that the person making the SAR was not entitled to receive the information requested.

Relevant provisions in the legislation - See DPA 2018 sections 44, 45, 51, 167, 169, and 173

External link

Further reading – ICO guidance

- Regulatory Action Policy
- Contracts and liabilities between controllers and processors